Topics in Algebra: The Higman-Thompson Group $G_{2,1}$ and Beauville p-groups

Nathan Barker

Thesis submitted for the degree of
Doctor of Philosophy

School of Mathematics and Statistics
University of Newcastle upon Tyne
Newcastle upon Tyne
United Kingdom

August 2014

Acknowledgements

I am grateful to EPSRC and Newcastle University for funding this research.

Part I: I would like to thank Collin Bleak, Claas Röver, José Burillo, Andrew Duncan, Matt Brin and Francesco Matucci. Also, this would not have all been possible without the support and guidance of my main supervisor Sarah Rees, who I thank for her time and patience.

Part II: My thanks go to (my extended supervisors) Nigel Boston, Ben Fairbairn and Norbert Peyerimhoff, and Alina Vdovina for bringing me in on this fruitful project.

A non-subject specific thank you must go to Anthony Youd, Michael Beaty, Peter Jørgensen, Raf Bocklandt, Stefan Kolb, Oliver King and all the postgraduate students I have met who provided me with support over the course of my 3.5 years at Newcastle University.

I also wish to thank Mikhail Belolipetsky, Steve Pride, Ian Short, Ben Fairbairn and José Burillo for inviting me to give seminars at their respective universities and Jessica Laffoley for allowing me to spend my summer working on my corrections.

Finally, I must thank again my two supervisors Sarah Rees and Alina Vdoniva for their supervision over the past 3.5 years.

Abstract

This thesis consists of two parts.

Part I of this thesis is concerned with the Higman-Thompson group $G_{2,1}$. We review and apply Definitions, Lemmas and Theorems described in a series of lectures delivered by Graham Higman during a visit to the Australian National University from July 1973 to October 1973 on a family of finitely presented infinite groups $G_{n,r}$ for $n \geq 2$ and $r \geq 1$. This thesis will concentrate on the group $G_{2,1}$ (otherwise know as Thompson's group V).

We give a brief account of the history of the Higman-Thompson group $G_{2,1}$, we clarify the proof of the conjugacy problem for elements in quasi-normal form and we prove that the power conjugacy problem for the group $G_{2,1}$ is decidable.

Part II of this thesis concentrates on the existence and structure of mixed and unmixed Beauville p-groups, for p a prime. We start by exhibiting the first explicit family of mixed Beauville 2-groups and find the corresponding surfaces. We follow this up by exploring the method that was used to construct the family; this leads to further ramification structures for finite p-groups giving rise to surfaces isogenous to a higher product of curves. We finish by classifying the non-abelian Beauville p-groups of order p^3, p^4 and provide partial results for p-groups of order p^5 and p^6. We also construct the smallest Beauville p-groups for each prime p.

Contents

Part I

The Higman-Thompson Group $G_{2,1}$

Chapter 1

Introduction

In Part I, the work of Graham Higman [Hig74] is used to provide a detailed account of the many properties of Richard Thompson's group V. This work takes the universal algebra view of Thompson's group V, which we will refer to as the Higman-Thompson group $G_{2,1}$ throughout this thesis. Part of this work has been submitted to a refereed journal, [Bar11].

Aims of this work I

We begin Part I of this thesis with a review of two of three main ways elements of the Higman-Thompson group $G_{2,1}$ are viewed.

We start by describing the representation of elements of $G_{2,1}$ as the group of right-continuous bijections of the unit interval that maps dyadic rational numbers to dyadic rational numbers that are differentiable except at finitely many dyadic rational numbers and such that on each maximal interval in which the function is differentiable the function is linear with derivative a power of 2, originally outlined by Richard Thompson in [Tho].

We follow this by describing the representation of elements of $G_{2,1}$ as tree pairs (which was first given in [CFP96], although we will follow [BGG11] treatment of the topic).

Remark 1.0.1. We prefer to reference [Tho] as the first place the elements of $G_{2,1}$ are described as dyadic rearrangements, even though [CFP96] is the classical reference. We do this as the unpublished notes of Richard Thompson are now available online.

We now give a brief synopsis of the main results of Part I of this thesis. All concepts will be defined in due course in the appropriate chapters.

The start of Chapter 2 outlines the important concepts from Universal Algebra which will be needed in this part of the thesis. We use the work of [Cohn91, Chapter

1] to define Ω-algebras, congruences on Ω-algebras, free algebras and varieties of free algebras.

The main part of Chapter 2 is then devoted to the definition of the free algebra $V_{2,1}$, originally defined by Graham Higman in [Hig74]. We place the work of [Hig74, Section 2] in the context of the definitions from Sections 2.1-2.3. We follow this with a formal definition of the group $G_{2,1}$, as the algebra automorphism group of the free algebra $V_{2,1}$.

Chapter 2 concludes with the definitions of semi-normal and quasi-normal forms for elements of the group $G_{2,1}$.

Chapter 3 is devoted to decision problems for the group $G_{2,1}$. Specifically, conjugacy problems for elements given in quasi-normal form of the group $G_{2,1}$. The chapter starts by considering a general element ψ of $G_{2,1}$ and looking at two ψ-invariant subalgebras of $V_{2,1}$, Theorem 3.1.1. Theorem 3.1.1 gives the first condition for conjugacy between two elements of $G_{2,1}$.

Following this, a formal introduction to the classical decision problems of Dehn is given.

To put Chapter 3 into some context, we note that Graham Higman originally solved the conjugacy problem for the Higman-Thompson groups $G_{2,1}$ (in fact for the infinite family of finitely presented groups $G_{n,r}$, $n \geq 2, r \geq 1$, which we do not discuss here) in [Hig74, Section 9]. However, since this proof is acknowledged to be difficult, we have deconstructed Higman's proof into small lemmas, which we prove using Higman's original techniques. We start by proving a series of lemmas in Section 3.3.1 that give conditions for two elements of $G_{2.1}$ to be conjugate.

The work of [SD10] provides a different solution to the conjugacy problem for the Higman-Thompson group $G_{2,1}$, using the revealing tree pair representation of elements defined by Matt Brin [Brin04].

The first part of Section 3.3.1 is devoted to the conjugacy problem for regular infinite elements of $G_{2,1}$, the main result is the following.

Proposition 3.3.21: Let ψ and φ be regular infinite elements of $G_{2,1}$ in quasi-normal form with respect to X and Y respectively.

Then, ψ is conjugate to φ if and only if there exists a map $\rho_0 \in \mathcal{R}(\psi;\varphi)$ such that ρ_0 extends to an element ρ of $G_{2,1}$ with $\rho^{-1}\psi\rho = \varphi$.

The second part of Section 3.3.1 is devoted to the conjugacy problem for periodic elements of $G_{2,1}$, the main result is the following.

Proposition 3.3.6: Let ψ and φ be torsion elements of $G_{2,1}$ in quasi-normal form with respect to the bases X and Y respectively. Then, ψ is conjugate to φ if and only if ψ and φ have the same cycle type.

The work on the conjugacy problem for elements in quasi-normal form is concluded in Section 3.3.2, where an algorithm (Algorithm 3.3.25) is given. Thus, we have the following theorem (as originally proved in [Hig74, Section 9]).

Theorem 3.3.26:[Hig74, part of Theorem 9.3] The conjugacy problem is soluble in $G_{2,1}$.

The final part of Chapter 3 considers the power conjugacy problem for elements in quasi-normal form. The problem (Problem 3.4.1) is defined and the intermediate results rely on results of Section 3.3.1. An algorithm (Algorithm 3.4.12) is presented in Section 3.4.2 which leads to the following conclusion.

Theorem 3.4.13: The power conjugacy problem for the Higman-Thompson group $G_{2,1}$ is solvable.

1.1 Richard Thompson's Groups F, T and V

Richard J. Thompson in the late 1960s defined three new groups (of permutations of dyadic splittings of the unit interval) which he called $\mathbb{P}$ (Thompson's Group F), G (Thompson's Group T) and V, with very interesting properties.

In some unpublished notes [Tho] Thompson shows $\mathbb{P}$ is a finitely presented group that is isomorphic to $\widehat{\mathbb{P}}$, a non-abelian torsion-free infinite group generated by order preserving permutations of the unit interval $[0,1]$. We now present some of this unpublished material (which can now be found in the introductory article on Thompson's Groups F, T and V by Cannon, Floyd and Parry [CFP96]).

Let $\mathbb{P}$ be the group given by the presentation

$$\langle R_0, R_1 | [R_0^{-1}R_1, R_0R_1R_0^{-1}], [R_0^{-1}R_1, R_0^2R_1R_0^{-2}] \rangle \tag{1.1}$$

where $[x,y] = xyx^{-1}y^{-1}$. It can be shown that all proper quotient groups of $\mathbb{P}$ are abelian (see [CFP96, Theorem 4.3]).

We define $\widehat{\mathbb{P}}$ to be the group generated by the following permutations of the unit interval $[0,1]$,

$$\widehat{R}_0(x) = \begin{cases} \frac{1}{2}x, & \text{if } 0 \le x \le \frac{1}{2}, \\ x - \frac{1}{4}, & \text{if } \frac{1}{2} \le x \le \frac{3}{4}, \\ 2x - 1, & \text{if } \frac{3}{4} \le x \le 1. \end{cases} \quad \text{and} \quad \widehat{R}_1(x) = \begin{cases} x, & \text{if } 0 \le x \le \frac{1}{2}, \\ \frac{1}{4} + \frac{1}{2}x, & \text{if } \frac{1}{2} \le x \le \frac{3}{4}, \\ x - \frac{1}{8}, & \text{if } \frac{3}{4} \le x \le \frac{7}{8}, \\ 2x - 1, & \text{if } \frac{7}{8} \le x \le 1. \end{cases}$$

We note that $\widehat{R}_0\widehat{R}_1(x) \neq \widehat{R}_1\widehat{R}_0(x)$, so $\widehat{\mathbb{P}}$ is non-abelian. Furthermore, since $\widehat{\mathbb{P}}$ is a torsion-free non-trivial order preserving permutation group of the interval $[0,1]$, we see that $\widehat{\mathbb{P}}$ is infinite. The group $\widehat{\mathbb{P}}$ satisfies the relations given in the Presentation (1.1) and so $\widehat{\mathbb{P}}$ is isomorphic to a quotient group of $\mathbb{P}$. However, as $\widehat{\mathbb{P}}$ is non-abelian, $\widehat{\mathbb{P}}$ can only be isomorphic to $\mathbb{P}$.

To the presentation of the group $\mathbb{P}$, Presentation (1.1), we add a new generator C_1 and some extra relations

$$C_1 = R_1C_1R_0^{-1}R_1,\ R_0R_1R_0^{-1}R_1C_1R_0^{-1} = R_1R_1C_1R_0^{-1}R_0^{-1}R_1,$$

$$R_0C_1 = (R_1C_1R_0^{-1})^2 \text{ and } C_1^3 = 1$$

to create a new group G. Since $\mathbb{P}$ can be shown to be a subgroup of G (see [CFP96, Lemma 5.4]) this gives G as a finitely presented infinite group. Thompson identified G with the group $\widehat{\mathcal{C}}$ given by amending the presentation of $\widehat{\mathbb{P}}$ by adding the generator,

$$\widehat{C}_1(x) = \begin{cases} \frac{1}{2}x + \frac{3}{4}, & \text{if } 0 \leq x \leq \frac{1}{2}, \\ 2x - 1, & \text{if } \frac{1}{2} \leq x \leq \frac{3}{4}, \\ x - \frac{1}{4}, & \text{if } \frac{3}{4} \leq x \leq 1, \end{cases}$$

and the new relations

$$\widehat{C}_1 = \widehat{R}_1\widehat{C}_1\widehat{R}_0^{-1}\widehat{R}_1,\ \widehat{R}_0\widehat{R}_1\widehat{R}_0^{-1}\widehat{R}_1\widehat{C}_1\widehat{R}_0^{-1} = \widehat{R}_1\widehat{R}_1\widehat{C}_1\widehat{R}_0^{-1}\widehat{R}_0^{-1}\widehat{R}_1,$$

$$\widehat{R}_0\widehat{C}_1 = (\widehat{R}_1\widehat{C}_1\widehat{R}_0^{-1})^2 \text{ and } \widehat{C}_1^3 = 1.$$

It is then shown that $\widehat{\mathcal{C}}$ is a simple group and $G \cong \widehat{\mathcal{C}}$.

Furthermore, Thompson obtained the group $\widehat{V}$ by adjoining a new generator

$$\widehat{\pi}_1(x) = \begin{cases} \frac{1}{2}x + \frac{1}{2}, & \text{if } 0 \leq x \leq \frac{1}{2}, \\ 2x - 1, & \text{if } \frac{1}{2} \leq x \leq \frac{3}{4}, \\ x, & \text{if } \frac{3}{4} \leq x \leq 1, \end{cases}$$

and new relations to the presentation of the group $\widehat{\mathcal{C}}$. He then showed that $\widehat{V}$ is a simple group too. Thompson also stated that $\widehat{V}$ can be 2-generated and gave explicit generators, one of order 4 and another of order 6.

We note that multiplication of elements of the groups $\widehat{\mathbb{P}}$, $\widehat{\mathcal{C}}$ and $\widehat{V}$ is achieved by composition of functions.

We now make the formal definitions of the Thompson's groups F, T and V.

Definition 1.1.1 (Thompson's groups F, T and V)**.** We define F to be the group of

piecewise linear homeomorphisms of the closed interval $[0,1]$ to itself that are differentiable except at finitely many dyadic rational numbers and such that on intervals of differentiability the derivatives are powers of 2.

We define T to be the group of piecewise linear homeomorphisms of the circle S^1 (the interval $[0,1]$ with the endpoints 0 and 1 identified) to itself that map dyadic rational numbers to dyadic rational numbers, that are differentiable except at finitely many dyadic rational numbers and such that on intervals of differentiability the derivatives are powers of 2.

We define V to be the group of right-continuous bijections of the interval $[0,1]$ that map dyadic rational numbers to dyadic rational numbers, that are differentiable except at finitely many dyadic rational numbers and such that on each maximal interval on which the function is differentiable the function is linear with derivative a power of 2.

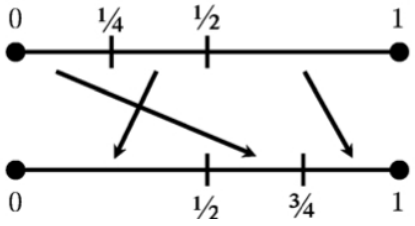
It was shown in [CFP96], that $F \cong \widehat{\mathbb{P}}$, $T \cong \widehat{\mathcal{C}}$ and $V \cong \widehat{V}$.

1.2 Tree pairs and Dyadic rearrangements

Taking the description of the group V in terms of right-continuous bijections of the interval $[0,1]$, Section 1.1, we can represent this group in a diagrammatic way. Many authors use a tree pair description. We follow the description of [Brin04, Section 10].

We will now describe elements of V as a pair of trees with a permutation.

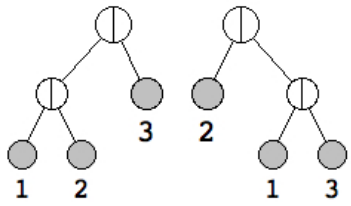
Figure 1.2.0.1: A dyadic rearrangement of the interval $[0,1]$ representing an element of V.



Let $\mathcal{J}$ be the set of finite words (including the empty word ϵ) on $\{0,1\}$. It is a monoid under concatenation (and in fact the free monoid on two generators) with the empty word ϵ as the identity.

Let $\mathcal{T}$ be the infinite binary tree. We can think of $\mathcal{J}$ as the set of nodes of $\mathcal{T}$ (we refer to elements of $\mathcal{J}$ as nodes of $\mathcal{T}$ when we do so) since we can think of $v0$ and $v1$ as the left and right child nodes of the node $v \in \mathcal{T}$. The empty word ϵ is the root of $\mathcal{T}$.

Figure 1.2.0.2: A tree pair representing figure 1.2.0.1 element of Thompson's Group V.



Definition 1.2.1. A dyadic *pattern* $\mathcal{P}$ on the unit interval I is a finite collection of ordered dyadic rational numbers (together with zero and one) *i.e.* $\mathcal{P} = \{0, x_1, ..., x_n, 1\}$ such that $x_i = \frac{a}{2^b}$ with b nonnegative integer and $a \leq 2^b - 1$ a nonnegative odd integer, for $i = 1, ..., n$ and $0 < x_1 \leq ... \leq x_n < 1$.

An *interval in a dyadic pattern* is the half open interval $[x_i, x_{i+1})$ for $x_i, x_{i+1} \in \mathcal{P}$ (except the final interval $[x_n, 1]$ for $x_n \in \mathcal{P}$).

Example 1.2.2. The finite collection $\{0, \frac{1}{4}, \frac{1}{2}, 1\}$ is the dyadic pattern associated to the first interval splitting in Figure 1.2.0.1 with intervals $[0, \frac{1}{4})$, $[\frac{1}{4}, \frac{1}{2})$ and $[\frac{1}{2}, 1]$.

Definition 1.2.3. A *dyadic rearrangement* is a right continuous bijection $f : I \to I$ that maps intervals of one dyadic pattern to another.

From the above definition, it is clear that Thompson's group V can be seen to be the group of all dyadic rearrangements of the unit interval $[0, 1]$.

Each node in $\mathcal{T}$ corresponds to an interval in a dyadic pattern on I. Recursively ϵ corresponds to I itself and if v corresponds to $[a, b)$, then $v0$ corresponds to $[a, c)$ and $v1$ corresponds to $[c, b)$ where $c = (a + b)/2$.

Here, a *finite binary tree* will be a finite subset D of $\mathcal{T}$ so that

1. every prefix of a node in D is also in D;

2. for all nodes v in D, $v0$ is in D if and only if $v1$ is in D.

We will refer to finite binary trees simply as finite trees, when the meaning is clear.

The *leaves* of such a D will be the nodes in D whose children are not in D. Nodes of a tree that are not leaves are called *interior nodes of a tree*. The root of every tree is the empty word ϵ.

The leaves of a finite tree D give a dyadic pattern in I by taking the intervals in I corresponding to the leaves of D. Two trees D and R (domain and range) with the same number, n, of leaves define two dyadic patterns in I with the same number of

intervals. If we are given a one-to-one correspondence between the leaves of D and the leaves of R, then we can build a right continuous bijection from $[0,1]$ to itself.

We now think of elements of Thompson's group V as triples $[D,R,\sigma]$ where D and R are finite trees with the same number, n, of leaves and where σ is a bijection from the leaves of D to the leaves of R. An example[1] is given in figure 1.2.0.2.

We will return to tree pairs in Chapter 5, where we will discuss a particular form representing tree pairs for an element of Thompson's group V.

Remark 1.2.4. From now on we will refer to Thompson's group V as the Higman-Thompson group $G_{2,1}$.

[1]This graphic was generated by a java scripted program, created by Roman Kogan. Further tree pairs given in this thesis are created using the LaTeX package `qtrees`.

Chapter 2

Universal Algebra and the Higman-Thompson group $G_{2,1}$

Graham Higman in [Hig74] gave a representation of Thompson's group V as the automorphism group of a free algebra in a variety of a particular class of free algebras. We will now introduce the concepts of free algebra and variety of free algebras, which come from Universal Algebra.

We start by introducing the terminology of operations on sets, definitions of Ω-algebra and Ω-subalgebra (in the sense of [Cohn91, Chapter 1], which we follow closely throughout Sections 2.1-2.3). We follow this with a definition of congruence on an Ω-algebra which then leads to a definition of free algebra and variety of free algebras.

This set up will then be used in Section 2.4, where the free algebra corresponding to the construction from Graham Higman [Hig74] gives rise to the Higman-Thompson group $G_{2,1}$.

2.1 Ω-algebra

For any integer $n \geq 0$ we define an *n-ary operation* on a set S to be a mapping of S^n into S. The number n is called the *arity* of the operation. A *finitary operation* is defined to be a mapping which is n-ary for some $n \in \mathbb{N}_0$ (the natural numbers together with zero).

Remark 2.1.1. We say *unary* for 1-ary and *binary* for 2-ary. A 0-ary operation on S is just a specific element of S, sometimes called a *constant* operation on S.

An *algbera* $\mathcal{A}$ here is thought of as a set S with certain finitary operations defined on it. In order to compare different algebras, we need to establish a correspondence between their sets of operations. This is achieved by indexing the operations in each

algebra by a given index set. An element of the set of operations is called an *operator* and has a given arity.

Definition 2.1.2. An *operator domain* is a set Ω and a mapping $a : \Omega \to \mathbb{N}_0$. The elements of Ω are called *operators*; if $\omega \in \Omega$, then $a(\omega)$ is called the *arity* of ω. We shall write $\Omega(n) = \{\omega \in \Omega | a(\omega) = n\}$, and refer to the members of $\Omega(n)$ as n-ary operations.

An Ω-algebra is defined as a pair (S, Ω) consisting of a set S with a family of operations indexed by Ω:

$$\omega : S^n \to S \quad \text{for each } \omega \in \Omega(n), \text{ n=0,1,2,... .} \tag{2.1}$$

The set S is called the *carrier* of the algebra and the set Ω is called the operator domain or the *signature* of the algebra.

Strictly speaking, we should denote the algebra by (S, Ω, φ), where φ is the family of mappings $\varphi_n : \Omega(n) \to Map(S^n, S)$ defined by (2.1), but usually we shall not distinguish notationally between an algebra and its carrier.

We now give an example, which we will refer back to throughout Sections 2.1-2.3.

Example 2.1.3 (Groups)**.** A *group* $(G, \cdot, ^{-1}, 1)$ is given by a binary operation (multiplication, $\cdot$), a unary operation (inversion, $^{-1}$) and a constant operation (the neutral element 1), satisfying certain laws.

Given an Ω-algebra (S, Ω) and $f \in \Omega$ with arity n, we can apply f to any n-tuple $s_1, ..., s_n \in S$ and obtain another element of S, which is written $s_1 ... s_n f$. In the case $n = 0$, we just single out an element of S, denoted by f.

We say that a subset $T \subseteq S$ is *closed under the operations of* Ω if for all f (of arity n) in Ω and for all $s_1, ..., s_n \in T$ the element $s_1 ... s_n f$ is also an element of T.

Definition 2.1.4. Given an Ω-algebra (S, Ω), an Ω-subalgebra is an Ω-algebra (S', Ω) whose set S' is a subset of S which is closed under the operations of Ω, as defined in S *i.e.* S' is Ω-closed.

We can clearly see that the intersection of any family of subalgebras is again a subalgebra. Hence, for any subset X of the set S we can form the intersection of all subalgebras containing X. This is called the subalgebra of (S, Ω) *generated* by X.

The subalgbera of (S, Ω) generated by X may also be formed by applying the operations of Ω to X and repeating this operation a finite number of times. If the subalgebra generated by X is the whole of S, then X is called a *generating set* for S.

A mapping $g : \mathcal{A} \to \mathcal{B}$ between two Ω-algebras $\mathcal{A} = (S, \Omega), \mathcal{B} = (S', \Omega)$ is said to be *compatible* with $f \in \Omega$ of arity n if for all $s_1, ..., s_n \in S$,

$$(s_1 g) ... (s_n g) f = (s_1 ... s_n f) g.$$

If g is compatible with each $f \in \Omega$, it is called a *homomorphism* from $\mathcal{A} = (S, \Omega)$ to $\mathcal{B} = (S', \Omega)$. If a homomorphism g from $\mathcal{A}$ to $\mathcal{B}$ has an inverse g^{-1} which is again a homomorphism, g is called an *isomorphism* and then the Ω-algebras $\mathcal{A} = (S, \Omega), \mathcal{B} = (S', \Omega)$ are said to be *isomorphic*.

An isomorphism of an algebra $\mathcal{A} = (S, \Omega)$ with itself is called an *automorphism* and a homomorphism of an algebra into itself is called an endomorphism.

A homomorphism is determined once it is known on a generating set, as stated in the next proposition (without proof).

Proposition 2.1.5. *([Cohn91, Proposition 1.1]) Let $g, h : \mathcal{A} \to \mathcal{B}$ be two homomorphisms between Ω-algebras $\mathcal{A} = (S, \Omega), \mathcal{B} = (S', \Omega)$. If g and h agree on a generating set, then they are equal.*

We now introduce the notion of direct product of Ω-algebras, in preparation for the next section on congruences on an Ω-algebra.

From a family $\{\mathcal{A}_i\}_{i=1}^m$ ($\mathcal{A}_i = (S_i, \Omega)$) of Ω-algebras we can form the *direct product* $P = \prod_{i=1}^m \mathcal{A}_i$ of Ω-algebras. Its set is the Cartesian product S of the S_i, and the operations are carried out componentwise. Thus, if $\pi_i : S \to S_i$ are the projections from the product to the factors then any $f \in \Omega$ of arity n is defined on S^n by the equation

$$(p_1 ... p_n f)\pi_i = (p_1\pi_i)...(p_n\pi_i)f,$$

where $p_i \in S$.

Let $\mathcal{C}$ be a class of Ω-algebras, whose elements we will call $\mathcal{C}$-algebras. By a *free $\mathcal{C}$-algebra* on a set X we mean a $\mathcal{C}$-algebra F in $\mathcal{C}$ with the following universal property:

there is a mapping $\mu : X \to F$ such that every mapping $f : X \to \mathcal{A}$ into a $\mathcal{C}$-algebra $\mathcal{A}$ can be factored uniquely by μ to give a homomorphism from F to $\mathcal{A}$, *i.e.* there exists a unique homomorphism $f' : F \to \mathcal{A}$ such that $\mu f' = f$. It is worth noting that Theorem 2.3.3 shows that $W_\Omega(X)$ is the free algebra on X in the class of all Ω-algebras.

Not every class has free algebras, but they exist in some cases as we will see in Proposition 2.3.6.

A *free product* is defined in a similar way, replacing the set X by a collection of $\mathcal{C}$ algebras. Given an indexing set I and for each $i \in I$ an Ω algebra A_i from $\mathcal{C}$ the free product $\mathcal{A}$ of $\{A_i\}_{i \in I}$, written $\mathcal{A} = *_{i \in I} \mathcal{A}_i$, is an Ω-algebra in $\mathcal{C}$ satisfying the following property.

There exists mappings $\mu_i : A_i \to \mathcal{A}$, for all $i \in I$, such that for any Ω-algebra $\mathcal{B}$ and family of mappings $f_i : A_i \to \mathcal{B}$, for all $i \in I$, there exists a unique homomorphism $f' : \mathcal{A} \to \mathcal{B}$ such that $\mu_i f' = f_i$ for all i.

Given collections $\{\mathcal{A}_i\}_{i\in I}$ and $\{\mathcal{B}_i\}_{i\in I}$ of Ω-algebras such that there exists free products $\mathcal{A} = *_{i\in I}\mathcal{A}_i$, $\mathcal{B} = *_{i\in I}\mathcal{B}_i$, then the definition above gives maps $\mu_i : \mathcal{A}_i \to \mathcal{A}$, $\mu_i' : \mathcal{B}_i \to \mathcal{B}$ for all $i \in I$. Suppose there exists homomorphisms $f_i : \mathcal{A}_i \to \mathcal{B}_i$ for all $i \in I$. Then $f_i\mu_i'$ is a homomorphism from $\mathcal{A}_i$ to $\mathcal{B}$ for all $i \in I$ so there exists a unique homomorphism $f' : \mathcal{A} \to \mathcal{B}$ with $\mu_i f' = f_i\mu_i'$ for all $i \in I$. We denote f' by $*_{i\in I}f_i$.

2.2 Congruence on an Ω-algebra

The main objective of this section is to define what is meant by a "congruence on an Ω-algebra."

Firstly, a *correspondence* between any two sets S and R is defined to be a subset of the Cartesian product $S \times R$.

Definition 2.2.1. Let S and R be any sets. A *mapping* $f : S \to R$ is a correspondence $\Gamma_f \subset S \times R$ with the following properties:

- (everywhere defined) for each $s \in S$ there exists $r \in R$ such that $(s, r) \in \Gamma_f$,
- (single-valued) if $(s, r), (s, r') \in \Gamma_f$ then $r = r'$.

We now define two operations on correspondences. For any correspondence $\Gamma \subset S \times R$ we have the inverse, defined as

$$\Gamma^{-1} = \{(r, s) \in R \times S | (s, r) \in \Gamma\};$$

next, if $\Gamma \subset S \times R$ and $\Delta \subset R \times T$, then their composition is given by

$$\Gamma \circ \Delta = \{(s, t) \in S \times T | (s, x) \in \Gamma \text{ and } (x, t) \in \Delta \text{ for some } x \in R\}.$$

If $\Gamma \subset S \times R$ and $S' \subset S$ we define

$$S'\Gamma = \{r \in R | (s, r) \in \Gamma \text{ for some } s \in S'\}.$$

There are two natural correspondences one can define. On every set S there is the *identity correspondence* $1_S = \{(s, s) | s \in S\}$ and the *universal correspondence* $S^2 = \{(s, s') | s, s' \in S\}$.

Definition 2.2.2. An *equivalence* on S is a subset Γ of S^2 with the properties

1. (transitivity) $\Gamma \circ \Gamma \subset \Gamma$,
2. (symmetry) $\Gamma^{-1} = \Gamma$,
3. (reflexivity) $1_S \subseteq \Gamma$.

The *equivalence class* of $s \in S$ is $\{s' \in S | (s, s') \in \Gamma\} = \{s\}\Gamma$.

Given any subset U of $S \times S$, the *equivalence generated* by U is the smallest equivalence E on S containing U. It can be seen that

$$E = \bigcap \{V \subseteq S \times S | V \text{ is an equivalence and } U \subseteq V\}.$$

Also, it follows that E is

$$\{(a, b) \in S \times S | \text{there exists } a_0, ..., a_n \text{ such that } a_0 = a,\ a_n = b \text{ and } (a_i, a_{i+1}) \in U\}.$$

To use correspondences in the study of Ω-algebras, we need to know their behavior as subalgebras. Firstly, if $\mathcal{A} = (S, \Omega)$ and $\mathcal{B} = (R, \Omega)$ are Ω-algebras and $\Gamma \subset S \times R$ is a correspondence which is closed under the operations of Ω, as defined in $\mathcal{A} \times \mathcal{B}$, then (Γ, Ω) is a subalgebra of $\mathcal{A} \times \mathcal{B}$. In this case we abuse notation and say Γ is a subalgebra of $\mathcal{A} \times \mathcal{B}$.

Lemma 2.2.3. *([Cohn91, Lemma 2.1, Chapter 1]) Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be Ω-algebras and let Γ, Δ be subalgebras of $\mathcal{A} \times \mathcal{B}, \mathcal{B} \times \mathcal{C}$ respectively. Then Γ^{-1} is a subalgebra of $\mathcal{B} \times \mathcal{A}$, $\Gamma \circ \Delta$ is a subalgebra of $\mathcal{A} \times \mathcal{C}$ and for any subalgebra $\mathcal{A}'$ of $\mathcal{A}$, $\mathcal{A}'\Gamma$ is a subalgebra of $\mathcal{B}$.*

Let S and T be any sets and $f : S \to T$ a mapping between them. Then the *image* of f is defined as $S\Gamma_f$, also written $\mathrm{im}f$; the *kernel* of f is defined as the correspondence

$$\ker f = \{(x, y) \in S^2 | xf = yf\}.$$

This is an equivalence on S; the different equivalence classes are just the inverse images of elements in the image (sometimes called the fibres of f).

Example 2.2.4 (Groups)**.** If we look at the definition of the kernel above of then we can relate it to the kernel of a homomorphism of groups. Given a group homomorphism $f : G \to H$, the kernel of f is the inverse image under f of the unit element of H. This is a normal subgroup N of G and the different cosets of N in G are just the fibres of f.

So, the equivalence classes of $\ker f$ from the definition above, are the cosets of N in G.

Let S and T be any sets and Γ a correspondence from S to T. The correspondence Γ will be used to define a system of subsets of S, T.

For any subset X of S we define a subset X^* of T by

$$X^* = \{y \in T | (x, y) \in \Gamma \text{ for all } x \in X\} = \cap_{x \in X} \{x\}\Gamma,$$

and similarly, for any subset Y of T we define a subset Y^* of S by

$$Y^* = \{x \in S | (x, y) \in \Gamma \text{ for all } y \in Y\} = \cap_{y \in Y} \{y\}\Gamma^{-1}.$$

We thus have mappings $X \mapsto X^*$ and $Y \mapsto Y^*$ of the power sets of S and T with the following properties:

$$X_1 \subseteq X_2 \Rightarrow X_1^* \supseteq X_2^*,\ Y_1 \subseteq Y_2 \Rightarrow Y_1^* \supseteq Y_2^*, \tag{2.2}$$

$$X \subseteq X^{**},\ Y \subseteq Y^{**}, \tag{2.3}$$

$$X^{***} = X^*,\ Y^{***} = Y^*. \tag{2.4}$$

A pair of mappings $X \mapsto X^*$ and $Y \mapsto Y^*$ between the power sets of S and T satisfying (2.2-2.4) is called a *Galois connexion*.

A *congruence* on an Ω-algebra $\mathcal{A} = (S, \Omega)$ is an equivalence on S which is also a subalgebra of $\mathcal{A}^2$ *i.e.* an equivalence $\Gamma \subset S \times S$ which is Ω-closed. From the above, $1_{\mathcal{A}}$ and $\mathcal{A}^2$ are congruences on $\mathcal{A}$.

Given any subset $U \subseteq S \times S$ the *congruence generated by* U is

$$C = \bigcap \{V |\ V \text{ is a congruence and } U \subseteq V\}.$$

It follows that C is the smallest congruence on $\mathcal{A}$ containing U.

Let $\mathcal{A}$ be an Ω-algebra. By definition a congruence is an equivalence which admits the operations ω ($\omega \in \Omega(n)$). Now each n-ary operator ω defines an n-ary operation on $\mathcal{A}$:

$$(a_1, ..., a_n) \to a_1 ... a_n \omega \text{ for } a_1, ..., a_n \in \mathcal{A}. \tag{2.5}$$

By giving fixed values in $\mathcal{A}$ to some of the arguments, we obtain r-ary operations for $r \leq n$; in particular, if we fix all the a_i except one, $x \in \mathcal{A}$, we obtain for any $n-1$ elements $a_1, ..., a_{n-1} \in \mathcal{A}$ and any $i = 1, ..., n$ a unary operation

$$x \to a_1 ... a_{i-1} x a_i ... a_{n-1} \omega. \tag{2.6}$$

We say that the operation (2.6) is an *elementary translation* derived from (2.5) by specialisation in $\mathcal{A}$.

Proposition 2.2.5. *([Cohn81, Proposition 6.1, Chapter6] An equivalence* $\mathfrak{q}$ *on an* Ω*-algebra* $\mathcal{A}$ *is a congruence if and only if it admits all translations; more precisely, a congruence admits all translations, while any equivalence admitting all elementary translations is a congruence.*

Remark 2.2.6. If $U \subseteq S \times S$, then the congruence generated by U can be seen to consist of pairs $(a, b) \in S \times S$ such that there exists $a_0, ..a_m$, $a_i \in S$ with $n \geq 0$, with

- $a_0 = a$, $a_m = b$
- $(a_i, a_{i+1}) = (u_i\tau, u_{i+1}\tau)$

where τ is an elementary translation (including $\tau =$ Identity) and $(u_i, u_{i+1}), (u_{i+1}, u_i) \in U$. *i.e.* there exists $s_1, ..., s_{n-1} \in S$, $u \in S$, $0 \leq j \leq m$ and $\omega \in \Omega(n)$ such that

$$u\tau = (s_1, ..., s_{j-1}u, s_j, ..., s_{n-1})\omega$$

so

$$a_i = (s_1, ..., s_{j-1}u_i, s_j, ..., s_{n-1})\omega,$$

$$a_{i+1} = (s_1, ..., s_{j-1}u_{i+1}, s_j, ..., s_{n-1})\omega$$

(or $a_i = u_i$, $a_{i+1} = u_{i+1}$) with $(u_i, u_{i+1}), (u_{i+1}, u_i) \in U$.

The next two theorems explain the significance of congruences for Ω-algebras and will be used in the following section on free algebras and varieties.

Theorem 2.2.7. *([Cohn91, Theorem 2.2, Chapter 1]) Let $g : \mathcal{A} \to \mathcal{B}$ be a homomorphism of Ω-algebras. Then imf is a subalgebra of $\mathcal{B}$ and $kerf$ is a congruence on $\mathcal{A}$.*

For any congruence $\mathfrak{q}$ on $\mathcal{A}$, we define an algebra structure, denoted $\mathcal{A}/\mathfrak{q}$, such that the natural mapping $\mathcal{A} \to \mathcal{A}/\mathfrak{q}$ is a homomorphism with kernel $\mathfrak{q}$. This is formalized in the following theorem.

Theorem 2.2.8. *([Cohn91, Theorem 2.3, Chapter 1]) Let $\mathcal{A}$ be an Ω-algebra and $\mathfrak{q}$ a congruence on $\mathcal{A}$. Then, there exists a unique Ω-algebra, denoted $\mathcal{A}/\mathfrak{q}$, with carrier the set of all $\mathfrak{q}$-classes such that the natural mapping $\nu : \mathcal{A} \to \mathcal{A}/\mathfrak{q}$ is a homomorphism.*

The algebra $\mathcal{A}/\mathfrak{q}$ is called the *quotient algebra* of $\mathcal{A}$ by $\mathfrak{q}$, with the *natural homomorphism* $\nu : \mathcal{A} \to \mathcal{A}/\mathfrak{q}$.

Example 2.2.9 (Group)**.** Given a group G with a normal subgroup N, we can put a group structure on the set G/N (the quotient group) such that the natural mapping $G \to G/N$ is a homomorphism.

2.3 Free algebras and varieties

To study Ω-algebras one needs to form expressions in indeterminates. Let $X = \{x_1, x_2, ...\}$ be any set, called an *alphabet*, and Ω any operator domain, with $\Omega \cap X = \emptyset$.

We define an Ω-algebra as follows: An Ω-row in X is a finite sequence of elements in the set $\Omega \cup X$. The set of all Ω-rows in X is denoted $W(\Omega; X)$. The length of an

Ω-row $w \in W(\Omega; X)$ is written $|w|$ and is the number of terms in w *i.e.* if $w = w_1...w_m$ where $w_i \in \Omega \cup X$ then $|w| = m$. We define an action of Ω on $W(\Omega; X)$ by juxtaposition; thus if $f_i \in \Omega$, of arity n_i, and $u_1, ..., u_{n_i} \in W(\Omega; X)$, then the effect of f_i on the n_i-tuple $(u_1, ..., u_{n_i})$ is the row $u_1...u_{n_i}f_i$. That is to say that the carrier S of our Ω-algebra is $W(\Omega; X)$, the set of Ω-rows. By abuse of notation we will refer to $W(\Omega; X)$ as an Ω-algebra.

It is clear that $X \subset W(\Omega; X)$ and we call the subalgebra generated by X the Ω-*word algebra* on X, denoted by $W_\Omega(X)$. Its elements are Ω-*words* in the alphabet X.

There is a clear distinction between Ω-rows which are Ω-words and those that are not. For example, if there is one binary operation f, then

$$x_1x_2x_3fx_4ff = (x_1, ((x_2, x_3)f, x_4)f)f$$

is a Ω-row which is also an Ω-word while $x_1ffx_2fx_3$ is an Ω-row which is not an Ω-word.

Definition 2.3.1. ([Cohn91, Chapter 1]) We define the *valency* of an Ω-row $w = w_1...w_m$ ($w_i \in \Omega \cup X$) as $v(w) = \sum_{i=1}^{m} v(w_i)$ where

$$v(w_i) = \begin{cases} 1, & \text{if } w_i \in X, \\ 1 - n_i, & \text{if } w_i \in \Omega, \text{ of arity } n_i. \end{cases}$$

Proposition 2.3.2. *([Cohn91, Proposition 3.1, Chapter 1]) An Ω-row $w = w_1...w_m$ in $W(\Omega; X)$ is an Ω-word if and only if every left-hand factor $u_i = w_1...w_i$ of w satisfies*

$$v(u_i) > 0 \text{ for } i = 1, ..., m,$$

and

$$v(w) = 1.$$

Moreover, each word can be obtained in just one way from its constituents.

Let $\mathcal{A}$ be an Ω-algebra. If in an element w of $W_\Omega(X)$ we replace each element of X by an element of $\mathcal{A}$ we obtain a unique element of $\mathcal{A}$. For $|w| = 1$, this is clear, so assume $|w| > 1$ and we will use induction on the length of w. We have $w = u_1...u_{n_i}f_i$ ($f_i \in \Omega$, $u_i \in W_\Omega(X)$), where the u_i are uniquely determined once w is given, by Proposition 2.3.2. By induction each u_i becomes $a_i \in \mathcal{A}$ when we replace the elements of X by elements of $\mathcal{A}$, hence w becomes $a_1...a_{n_i}f_i$ which is another element of $\mathcal{A}$.

This leads to the universal property of the Ω-word algebra, that is that $W_\Omega(X)$ is the free Ω-algebra on X, freely generated by X.

Theorem 2.3.3. *([Cohn91, Theorem 3.2, Chapter 1]) Let $\mathcal{A}$ be an Ω-algebra and X a set. Then any injective mapping $\theta : X \to \mathcal{A}$ extends in just one way to a homomorphism $\bar{\theta} : W_\Omega(X) \to \mathcal{A}$.*

Given any Ω-algebra $\mathcal{A}$, we can take a generating set X of $\mathcal{A}$ and apply the construction of Theorem 2.3.3 to give the corollary below.

Corollary 2.3.4. *([Cohn91, Corollary 3.3, Chapter 1]) Any Ω-algebra $\mathcal{A}$ can be expressed as a homomorphic image of an Ω-word algebra $W_\Omega(X)$ for a suitable set X. Here X can be taken to be any set corresponding to a generating set of $\mathcal{A}$.*

When we come to define a concrete class of algebras, we do so by specifying its operations $f_i \in \Omega$, a set S and equations holding identically for all elements of S. Generally, by an *identity* or *law* over Ω in X we mean a pair $(u, v) \in W_\Omega(X) \times W_\Omega(X)$ or an equation formed from the pair $u = v$. We say that the law (u, v) *holds* in the Ω-algebra $\mathcal{A}$ or that $\mathcal{A}$ *satisfies* the equation $u = v$ if every homomorphism $W_\Omega(X) \to \mathcal{A}$ maps u and v to the same element of $\mathcal{A}$.

This relation between sets of laws and classes of algebras establishes a Galois connexion.

- Given any set Σ of laws, we can form $\mathcal{V}_\Omega(\Sigma)$, the class of all Ω-algebras satisfying all the laws in Σ. This class $\mathcal{V}_\Omega(\Sigma)$ is called the *variety* generated by Σ.

- Given a class $\mathcal{C}$ of Ω-algebras we can form the set $\mathfrak{q} = \mathfrak{q}(\mathcal{C})$ of all laws which hold in all algebras of $\mathcal{C}$.

This Galois connexion relates each variety of Ω-algebras to a correspondence $\mathfrak{q}$ on $W_\Omega(X)$, which is also a congruence.

A subalgebra of an Ω-algebra $\mathcal{A}$ is called *fully invariant* if it is mapped into itself by all endomorphisms of $\mathcal{A}$. This definition also extends to congruences Γ on $\mathcal{A}$, viewed as subalgebras of $\mathcal{A}^2$. The *fully invariant congruence generated by* Γ is

$$C = \bigcap \{V |\ V \text{ is a fully invariant congruence and } \Gamma \subseteq V\}.$$

It follows that C is the smallest invariant congruence on $\mathcal{A}$ generated by Γ.

The congruence properties of $\mathfrak{q}(\mathcal{C})$ are shown in the following way: in every class $\mathcal{C}$ of Ω-algebras we have $u = u$ for any $u \in W_\Omega(X)$. If $u = v$ holds then so does $v = u$ and if $u = v, v = w$ then $u = w$ holds too. Further, if $u_i = v_i$ for $i = 1, ..., n$ are laws holding in $\mathcal{A}$ and $\omega \in \Omega$ of arity n, then $u_1 ... u_n \omega = v_1 ... v_n \omega$ holds in $\mathcal{A}$.

To show that $\mathfrak{q}(\mathcal{C})$ is a fully invariant congruence, let $(u, v) \in \mathfrak{q}(\mathcal{C})$ and let θ be any endomorphism of $W_\Omega(X)$. If $\alpha : W_\Omega(X) \to \mathcal{A}$, where $\mathcal{A} \in \mathcal{C}$, is any homomorphism,

then so is $\theta\alpha$, hence $u\theta\alpha = v\theta\alpha$. Thus the law $u\theta = v\theta$ holds in $\mathcal{A}$, so $(u\theta, v\theta) \in \mathfrak{q}(\mathcal{C})$ and this shows that $\mathfrak{q}(\mathcal{C})$ is a fully invariant congruence.

Theorem 2.3.5. *([Cohn91, Theorem 3.5, Chapter 1]) Let $W = W_\Omega(X)$ be the Ω-word algebra on an infinite alphabet X. Then the Galois connexion between Ω-algebras and laws establishes a natural bijection between varieties of Ω-algebras and fully invariant congruences on W.*

That is:

$$\{\text{Varieties of } \Omega\text{-algebras}\} \longleftrightarrow \{\text{Fully invariant congruences on } W_\Omega(X)\}.$$

Free algebras exist in varieties.

Proposition 2.3.6. *([Cohn91, Proposition 3.6, Chapter 1]) Let $\mathcal{V}$ be a variety of Ω-algebras and $\mathfrak{q}$ the congruence on $W_\Omega(X)$ (the Ω-word algebra generated by X) consisting of all the laws on $\mathcal{V}$* i.e. *the fully invariant congruence $\mathfrak{q}(\mathcal{V})$. Then $W_\Omega(X)/\mathfrak{q}$ is the free $\mathcal{V}$-algebra on X.*

Suppose Σ is a set of laws over Ω in X and let $\mathcal{V} = \mathcal{V}_\Omega(\Sigma)$ and $\mathfrak{q} = \mathfrak{q}(\mathcal{V})$. Then $\Sigma \subseteq \mathfrak{q}$ and, from Proposition 2.3.6, $\mathfrak{q}$ is a fully invariant congruence and $W_\Omega(X)/\mathfrak{q}$ is the free $\mathcal{V}$-algebra.

Now let $\mathfrak{p}$ be the fully invariant congruence generated by Σ. Then, as $\Sigma \subseteq \mathfrak{q}$ and $\mathfrak{q}$ is a fully invariant congruence, we have $\mathfrak{p} \subseteq \mathfrak{q}$. Let $A = W_\Omega(X)/\mathfrak{p}$. Then A is an Ω-algebra, in which every law of Σ holds (as $\Sigma \subseteq \mathfrak{p}$). Thus A is a $\mathcal{V}$-algebra. Then, from Proposition 2.3.6, the natural map $X \to A$ extends to a homomorphism $W_\Omega(X)/\mathfrak{q} \to A$. It follows that $\mathfrak{q} \subseteq \mathfrak{p}$. Therefore $\mathfrak{p} = \mathfrak{q} = \mathfrak{q}(\mathcal{V})$.

This argument above will be used to construct the Higman algebra in Section 2.4 using the fact that the equivalence relation generated by Σ (Definition 2.4.2) is a fully invariant congruence which is equal to $\mathfrak{q}(\mathcal{V}_\Omega(\Sigma))$.

2.4 The Higman Algebra $V_{2,1}$

We are now going to put Graham Higman's definition of his free algebra $V_{2,1}$ into the set-up of Sections 2.1-2.3. We will point out at each stage the parts of [Hig74, Section 2] we are referring to and the terminology that Graham Higman used.

We start with an Ω-algebra $\mathcal{A}$ with carrier S and operator domain $\Omega = \{\lambda, \alpha_1, \alpha_2\}$, with $a(\alpha_i) = 1$ for $i = 1, 2$ and $a(\lambda) = 2$.

We call the one binary operation λ,

$$\lambda : S^2 \to S$$

a *contraction* and the two unary operations,

$$\alpha_i : S \to S$$

descending operations, for $i = 1, 2$.

For any $v \in S$, we denote

$$v\alpha := (v\alpha_1, v\alpha_2).$$

Thus, α is a map,

$$\alpha : S \to S^2,$$

which we shall call an *expansion*. For any subset Y of S, a *simple expansion* of Y consists of substituting some element y of Y by the two elements of the tuple $y\alpha$. A series of d simple expansions of Y is called a *d-fold expansion of* Y. Similarly, a *simple contraction* of two distinct elements $\{y_1, y_2\}$ of Y consists of substituting $\{y_1, y_2\}$ by $(y_1, y_2)\lambda$.

We now define $W_\Omega(\{x\})$ to be the Ω-word algebra (with Ω as above). That is, $W_\Omega(\{x\})$ is the free Ω-algebra on the generating set $\{x\}$, freely generated by $\{x\}$ (see Section 2.3).

Remark 2.4.1. In the terminology that was used in [Hig74, Section 2], the set of *standard forms over* $\{x\}$ is a subset of the Ω-word algebra $W_\Omega(\{x\})$.

We shall now build a particular instance of the free algebra that Graham Higman defined in [Hig74] by considering a variety of Ω-algebras and using Proposition 2.3.6.

Definition 2.4.2. Let Σ be the following sets of laws,

1. for any $w \in W_\Omega(\{x\})$,
$$w\alpha\lambda = w,$$
(or explicitly $w\alpha_1 w\alpha_2\lambda = w$).
2. for any pair $(w_1, w_2) \in W_\Omega(\{x\})^2$,
$$w_1 w_2 \lambda\alpha_i = w_i \text{ for } i = 1, 2.$$

Let $\mathcal{V}_2$ be the variety of Ω-algebras which satisfy the laws in Σ (see Definition 2.4.2).

Definition 2.4.3. Let the $\mathfrak{q}$ be the congruence on $W_\Omega(\{x\})$ generated by the set

$$\begin{aligned} R_\Sigma = &\{(w\alpha_1 w\alpha_2\lambda, w) | w \in W_\Omega(\{x\})\} \\ &\cup \{(w_1 w_2 \lambda\alpha_1, w_1), (w_1 w_2 \lambda\alpha_2, w_2) | w_1, w_2 \in W_\Omega(\{x\})\}. \end{aligned}$$

From Proposition 2.3.6, and the comments following it, $\mathfrak{q}$ is the fully invariant congruence $\mathfrak{q}(\mathcal{V}_2)$ and $\mathcal{V}_2 = \mathcal{V}_\Omega(\Sigma) = \mathcal{V}_\Omega(\mathfrak{q})$. Moreover $W_\Omega(\{x\})/\mathfrak{q}$ is the free $\mathcal{V}_2$-algebra on $\{x\}$.

Remark 2.4.4. We now mention the work of [Hig74, Section 2]. Let $A = \{\alpha_1, \alpha_2\}$ and $V_{2,1}$ denote the free algebra of $\mathcal{V}_2$ freely generated by $\{x\}$. Graham Higman defines a *standard form over X* as one of the finite sequences of elements of $\{x\} \cup A \cup \{\lambda\}$ specified by the following rules:

(i) $x\alpha_{i_1}...\alpha_{i_k}$ is a standard form whenever $k \geq 0$ and $1 \leq i_j \leq 2$ for $j = 1, \ldots, k$.

(ii) If w_1, w_2 are standard forms, then so is $w_1 w_2 \lambda$ unless there is a standard form u such that $w_i = u\alpha_i$ for $i = 1, 2$.

(iii) No sequence is a standard form unless this follows from (i) and (ii).

Graham Higman made the set of standard forms into an Ω-algebra by defining the operations $\alpha_1, \alpha_2, \lambda$ as follows:

$$(x\alpha_{i_1}...\alpha_{i_k})\alpha_i = x\alpha_{i_1}...\alpha_{i_k}\alpha_i$$

$$(w_1 w_2 \lambda)\alpha_i = w_i$$

for $i = 1, 2$ and

$$(w_1, w_2)\lambda = w_1 w_2 \lambda$$

unless there is a standard form u such that $w_i = u\alpha_i$ for $i = 1, 2$ in which case Graham Higman defines

$$(w_1, w_2)\lambda = (u\alpha_1, u\alpha_2)\lambda = u.$$

Graham Higman then goes on to prove that the algebra of standard forms is a free algebra of $\mathcal{V}_2$, freely generated by $\{x\}$ ([Hig74, Lemma 2.1]). This is already given here by the set up from the previous sections (specifically Theorem 2.3.3 and Proposition 2.3.6).

Remark 2.4.5. By [Hig74, Corollary 2, page 12] (which states that $V_{n,r} \cong V_{n,s}$ if and only if $r \equiv s \mod n-1$) for $n = 2$ $V_{2,r} \cong V_{2,1}$, for all $r \geq 1$ and $r = |X|$, X a generating set.

Lemma 2.4.6. *Let $\{w\}^*$ be an equivalence class of elements of $W_\Omega(\{x\})$ given by the fully invariant congruence $\mathfrak{q}$. Then, there exists a unique minimal length element u in $\{w\}^*$. The unique minimal length elements of equivalence classes are precisely the standard forms of Higman.*

Proof. The proof depends on an explicit description of the congruence $\mathfrak{q}$. First define a *translation* to be a map τ from $W_\Omega(\{x\})^2$ given by one of the rules

$$\begin{aligned}
&(u,v)\tau = (u,v) \text{ or}\\
&(u,v)\tau = (u\alpha_i, v\alpha_i), i \in \{1,2\} \text{ or}\\
&(u,v)\tau = (uw\lambda, vw\lambda), w \in W_\Omega(\{x\} \text{ or}\\
&(u,v)\tau = (wu\lambda, wv\lambda), w \in W_\Omega(\{x\},
\end{aligned}$$

for all $(u,v) \in W_\Omega(\{x\})^2$.

Next, for $(u,v) \in W_\Omega(\{x\})^2$, we define *translation closure* of (u,v) to be the subset $\overline{(u,v)}$ of $W_\Omega(\{x\})^2$ with the following recursive definition. Namely, $\overline{(u,v)}$ is the smallest subset of $W_\Omega(\{x\})^2$ such that

1. $(u,v) \in \overline{(u,v)}$ and
2. if $(r,s) \in \overline{(u,v)}$ then $(r,s)\tau \in \overline{(u,v)}$ for all translations τ.

That is, $\overline{(u,v)}$ consists of the elements of $W_\Omega(\{x\})^2$ obtained by applying a finite sequence of translations to (u,v). Now define the *translation closure* $\bar{R}_\Sigma$ of R_Σ to be

$$\bar{R}_\Sigma = \bigcup_{(u,v)\in R_\Sigma} \overline{(u,v)}.$$

We claim that $\mathfrak{q}$ is the equivalence generated by $\bar{R}_\Sigma$. Temporarily denote this equivalence by $\mathfrak{p}$. As $\bar{R}_\Sigma$ is closed under translation it follows (see Proposition 2.2.5) that $\mathfrak{p}$ is a congruence; so $\mathfrak{p} \supseteq \mathfrak{q}$, as $\mathfrak{p} \supseteq R_\Sigma$. Furthermore, if $\mathfrak{p}'$ is a congruence containing R_Σ then $\mathfrak{p}'$ is closed under translation, so contains $\bar{R}_\Sigma$. Thus $\mathfrak{p}' \supseteq \mathfrak{p}$. In particular $\mathfrak{q} \supseteq \mathfrak{p}$, as required. Therefore $\mathfrak{q}$ is the equivalence generated by $\bar{R}_\Sigma$, as claimed.

Now we shall show that $\bar{R}_\Sigma$ has the following 2 properties. If $(a,b) \in \bar{R}_\Sigma$ then

(I) $|a| > |b|$ and

(II) there exist Ω-rows w_0 and w_1 in $W(\Omega, \{x\})$ and $(u,v) \in R_\Sigma$ such that $a = w_0uw_1$ and $b = w_0vw_1$.

If $(a,b) \in \bar{R}_\Sigma$ then (a,b) is obtained by applying a sequence of t translations to some $(u,v) \in R_\Sigma$. (I) and (II) are proved by induction on the number t of translations required. If $t = 0$ then $(a,b) \in R_\Sigma$ and I holds by definition of R_Σ and II holds with w_0 and w_1 trivial. Assume both these results hold for elements obtained by at most $t-1$ applications of translations, to an element of R_Σ. We have $(a,b) = (c,d)\tau$, for some translation τ and some $(c,d) \in \bar{R}_\Sigma$ which is obtained from (u,v) by $t-1$

applications of translations. From the inductive hypothesis $|c| > |d|$ and, since every translation changes the length of left and right hand sides of a pair by the same amount, it follows that $|a| > |b|$. Also, from the inductive hypothesis $c = w_0uw_1$ and $d = w_0vw_1$, for some Ω-rows w_0 and w_1. Depending on the type of τ we have $(a, b) = (c, d)$, or $(a, b) = (c\alpha_i, d\alpha_i) = (w_0uw_1\alpha_i, w_0vw_1\alpha_i)$ or $(a, b) = (w_0uw_1s\lambda, w_0vw_1s\lambda)$ or $(a, b) = (sw_0uw_1\lambda, sw_0vw_1\lambda)$, where $s \in W_\Omega(\{x\})$. In all cases (a, b) can be seen to have the form required by (II). By induction (I) and (II) hold for all (a, b).

We regard $\bar{R}_\Sigma$ as a reduction system on $W_\Omega(\{x\})$ (see for example [BO93]) and write $a \Longrightarrow b$ if $(a, b) \in \bar{R}_\Sigma$ and $a \overset{*}{\Longrightarrow} b$ if (a, b) is in the reflexive, transitive closure of $\bar{R}_\Sigma$. (Thus $a \overset{*}{\Longrightarrow} b$ if and only if $a = b$ or there is a seqence $a = a_0, \ldots, a_n = b$, such that $a_i \Longrightarrow a_{i+1}$.) As $\mathfrak{q}$ is the reflexive, symmetric, transitive closure of $\bar{R}_\Sigma$, the first statement of the lemma will follow if we show that $\bar{R}_\Sigma$ is

(a) terminating (every sequence $a_0 \overset{*}{\Longrightarrow} \cdots \overset{*}{\Longrightarrow} a_n \overset{*}{\Longrightarrow} \cdots$ is eventually stationary) and

(b) locally confluent: whenever $b \Longleftarrow a \Longrightarrow c$ there exists d such that $b \overset{*}{\Longrightarrow} d \overset{*}{\Longleftarrow} c$.

As $\bar{R}_\Sigma$ is length reducing it is certainly terminating, so we must show it is locally confluent. Before embarking on the proof of this fact, we consider the ways in which it is possible for words of $W_\Omega(\{x\})$ to overlap. To this end suppose that $p = ab$, and $q = bc$ are elements of $W_\Omega(\{x\})$, with b non-trivial. If a is non-trivial then we have $1 = v(p) = v(a) + v(b)$ and $v(a) \geq 1$, so $v(b) \leq 0$. However (see Proposition 2.3.2) this means that b must be trivial, a contradiction. Hence if p and q overlap then p is a subword of q or vice-versa. Assuming that q is a proper subword of p we then have $p = p_0qp_1$, where one of p_0, p_1 is non-trivial. If p_1 is non-trivial then $1 = v(p) = v(p_0q) = v(p_0) + v(q) = v(p_0) + 1$, so $v(p_0) = 0$, contradicting Proposition 2.3.2 again. We conclude that if p and q overlap and are not equal then one is a subword of the other and, assuming q is a subword of p,

$$p = p_0qp_1, \text{ with } p_1 \text{ non-trivial.} \tag{2.7}$$

Now suppose that $b \Longleftarrow a \Longrightarrow c$. From property (II) above, we have Ω-rows w_0, w_1, w_0' and w_1', and elements $(u, v), (r, s) \in R_\Sigma$, such that $(a, b) = (w_0uw_1, w_0vw_1)$ and $(a, c) = (w_0'rw_1', w_0'sw_1')$. If a factors as w_0uwrw_1' then setting $d = w_0vwsw_1'$ we have $b = w_0vwrw_1' \Longrightarrow d \Longleftarrow w_0uwsw_1' = c$, so local confluence holds in this case. Similarly, if $a = w_0'rwuw_1$ then we have local confluence. Assume then that a has no such factorisation. This means that u and r are overlapping subwords of a. Therefore, interchanging b and c if necessary, we may assume that r is subword of u. Thus, there exist Ω-rows p and q such that $u = prq$. We may therefore restrict to the case where

$a = u$, $b = v$ and $c = psq$. We consider in turn the various forms that u may take.

First consider the case $u = w\alpha_1 w\alpha_2\lambda$, for some $w \in W_\Omega(\{x\})$. Applying (2.7), r may be a subword of w in $w\alpha_1$, equal to $w\alpha_1$, a subword of w in $w\alpha_2$ or equal to $w\alpha_2$ (but may not begin in $w\alpha_1$ and end in wa_2). If r is a subword of w in $w\alpha_1$ then $u = w'rw''\alpha_1 w\alpha_2\lambda$, where $w = w'rw''$ and we have

$$b = w = w'rw'' \Longleftarrow u = w'rw''\alpha_1 w\alpha_2\lambda \Longrightarrow w'sw''\alpha_1 w\alpha_2\lambda = c$$

and then $c = w'sw''\alpha_1 w'rw''\alpha_2\lambda$ and $(w'sw''\alpha_1 w'sw''\alpha_2\lambda, w'sw'') \in R_\Sigma$ so

$$b = w'rw'' \Longrightarrow w'sw'' \Longleftarrow w'sw''\alpha_1 w'sw''\alpha_2\lambda \Longleftarrow c = w'sw''\alpha_1 w'rw''\alpha_2\lambda.$$

On the other hand if $u = rw\alpha_2\lambda$ with $r = w\alpha_1$ then $(r, s) \in R_\Sigma$ implies $w = w_1 w_2\lambda$ and $s = w_1$, so $c = sw\alpha_2\lambda = w_1 w_1 w_2\lambda\alpha_2\lambda$, for some $w_i \in W_\Omega(\{x\})$. In this case $sw\alpha_2 = w_1(w_1 w_2\lambda\alpha_2)\lambda \Longrightarrow w_1 w_2\lambda$,

$$b = w \Longleftarrow u = rw\alpha_2\lambda \Longrightarrow sw\alpha_2\lambda = c$$

and

$$b = w_1 w_2\lambda \Longleftarrow sw\alpha_2\lambda = c.$$

The cases where r is a subword of w in $w\alpha_2$ or r is equal to $w\alpha_2$ follow similarly.

Now consider the case where $u = w_1 w_2\lambda\alpha_i$, for $i = 1$ or 2. In this case r may be a subword of w_i, for $i = 1$ or 2, or r may equal $w_1 w_2\lambda$. In the latter case, $(r, s) \in R_\Sigma$ implies that $r = w\alpha_1 w\alpha_2\lambda$ and $s = w$. Thus we have $w\alpha_1 = v \Longleftarrow u = r\alpha_1 \Longrightarrow s\alpha_1 = w\alpha_1$, and there is nothing further to be proved. Suppose then that r is a subword of w_1, say $w_1 = w'rw''$. If $i = 1$ we have

$$b = w'rw'' \Longleftarrow u = w'rw''w_2\lambda\alpha_1 \Longrightarrow w'sw''w_2\lambda\alpha_1 = c$$

and

$$b = w'rw'' \Longrightarrow w'sw'' \Longleftarrow w'sw''w_2\lambda\alpha_1 = c.$$

If $i = 2$ then

$$b = w_2 \Longleftarrow u = w'rw''w_2\lambda\alpha_2 \Longrightarrow w'sw''w_2\lambda\alpha_2 = c$$

and

$$b = w_2 \Longleftarrow w'sw''w_2\lambda\alpha_2 = c.$$

The case where r is a subword of w_2 is similar. In all cases we have local confluence, so we conclude that (b) holds for $\bar{R}_\Sigma$. Therefore, (from [BO93, Section 1.1], for example) every equivalence class of $\mathfrak{q}$ contains a unique element which is not the left hand side

of any element of $\bar{R}_\Sigma$: such elements of $W_\Omega(\{x\})$ are called *irreducible* elements. As $\bar{R}_\Sigma$ is length reducing it follows that the unique irreducible element of an equivalence class is an element of minimal length in its equivalence class.

To prove the second statement of the Lemma note that every standard form is irreducible, so is of minimal length in its equivalence class. Conversely, given an irreducible element a straightforward induction on its length shows that it is a standard form. □

Definition 2.4.7. Let Y be a subset of $V_{2,1}$. A set Z obtained from Y by a finite number of simple expansions is called a *descendant* of Y.

Alternatively, Y is called an *ascendant* of Z if it can be obtained by a finite number of simple contractions from Z.

Example 2.4.8. A simple expansion of the free basis $\{x\}$ is given by the set $\{x\alpha_1, x\alpha_2\}$. There are two 2-fold expansions of $\{x\}$, they are $\{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2\alpha_2\}$ and $\{x\alpha_1\alpha_1, x\alpha_1\alpha_2, x\alpha_2\}$.

Lemma 2.4.9. *Any expansion of $\{x\}$ is a free basis of $V_{2,1}$.*

The proof uses the same arguments as the proof of [Hig74, Lemma 2.3]. In fact, we will show this by showing that if Y is an arbitrary expansion of $\{x\}$ that is a free basis of $V_{2,1}$, then a simple expansion of Y,

$$Y' = Y \setminus \{y\} \cup \{y\alpha_1, y\alpha_2\}$$

is also a free basis of $V_{2,1}$.

Proof. Let Y be an arbitrary expansion of $\{x\}$ and assume that Y is a (free) basis of $V_{2,1}$. Let

$$Y' = Y \setminus \{y\} \cup \{y\alpha_1, y\alpha_2\}.$$

Since $y = y\alpha_1 y\alpha_2 \lambda$, the set Y' generates $V_{2,1}$. We will show that Y' is a free basis of $V_{2,1}$.

Given $\mathcal{A} \in \mathcal{V}_2$ and a map $\theta : Y' \to \mathcal{A}$, then there is a unique homomorphism $\bar{\theta} : V_{2,1} \to \mathcal{A}$ extending θ.

Firstly, define θ^* from Y to $\mathcal{A}$ in the following way,

$$y'\theta^* = \begin{cases} y'\theta, & \text{for } y' \in Y \setminus \{y\}, \\ y'\alpha_1\theta y'\alpha_2\theta\lambda, & \text{otherwise.} \end{cases}$$

There is a unique homomorphism $\bar{\theta}^*$ from $V_{2,1}$ to $\mathcal{A}$ extending θ^*, since Y is a basis. Now

$$(y\alpha_i)\bar{\theta}^* = (y\bar{\theta}^*)\alpha_i = (y\theta^*)\alpha_i = (y\alpha_1\theta y\alpha_2\theta\lambda)\alpha_i = y\alpha_i\theta.$$

Hence $\bar{\theta}^*$ also extends θ.

Furthermore, any other map which extends θ must equal $\bar{\theta}^*$, since any such map must be defined on Y in the same way as θ^*. □

Remark 2.4.10. When I say basis, from now on I mean a basis which is an expansion of x.

Now that we have a concrete description of the free algebra $V_{2,1}$ in the variety $\mathcal{V}_2$, we can follow the work of Graham Higman in [Hig74, Section 2] and present some of the properties of the algebra $V_{2,1}$ (and its elements) that will be useful in future sections.

Definition 2.4.11. Let $A = \{\alpha_1, \alpha_2\} \subset \Omega$. We define $\langle A \rangle$ to be the free monoid $\{\alpha_1, \alpha_2\}^*$ and $\langle \lambda \rangle$ to be the free monoid on λ.

Definition 2.4.12. We write ϵ for the empty word in $\langle A \rangle$.

We first define two types of special subalgebras of $V_{2,1}$. We shall say that a subset U of $V_{2,1}$ is an *A-subalgebra* if there exists a basis Y of $V_{2,1}$ such that $U = Y\langle A \rangle$ *i.e.* every element of U is in some expansion of Y. Similarly, we say that a subset U of $V_{2,1}$ is an *λ-subalgebra* if there exists a basis Y of $V_{2,1}$ such that $U = Y\langle \lambda \rangle$ *i.e.* every element of U is some contraction of Y.

Remark 2.4.13. The above definitions are not an abuse of the definition of subalgebra (Definition 2.1.4), since each "subalgebra" U is closed under a subset of the operations from Ω.

Definition 2.4.14. We say that a subset U of $V_{2,1}$ is *A-closed* if it is closed under the operations of $A \subset \Omega$.

Let y be the minimal representative of its equivalence class in $V_{2,1}$ *i.e.* y is a standard form. Then the *λ-length* of y is the number of times the symbol λ occurs in y.

Below we give some examples of elements which are standard forms (that is minimal representatives of equivalence classes in $V_{2,1}$).

Example 2.4.15. The following elements are all standard forms: x, $x\alpha_2$, $x\Gamma$ (for $\Gamma \in \langle A \rangle$), $x\alpha_2 x\alpha_1\lambda$ (λ-length one), $x\alpha_2 x\lambda x\alpha_1^2\lambda$ (λ-length two). All standard forms of the form $x\Gamma$ for $\Gamma \in \langle A \rangle$ have λ-length zero.

A word $\Gamma \in \langle A \rangle$ is called *primitive* if it is not a power of another word; that is, if Γ (non-trivial) and $\Gamma \in \langle \Delta \rangle$ for $\Delta \in \langle A \rangle$ implies $\Gamma = \Delta$.

Proposition 2.4.16 ([Lot83], Proposition 1.3.1, Chapter 1). *If $\Gamma^n = \Delta^m$ with $\Gamma, \Delta \in \langle A \rangle$ and $n, m \geq 0$, there exists a word Λ such that $\Gamma, \Delta \in \langle \Lambda \rangle$.*

In particular, for each word $w \in \langle A \rangle$, there exists a unique primitive word Λ such that $w \in \langle \Lambda \rangle$.

Proposition 2.4.17 ([Lot83], Proposition 1.3.2, Chapter 1). *Two words $\Gamma, \Delta \in \langle A \rangle$ commute if and only if they are powers of the same word. More precisely the set of words commuting with a word $\Gamma \in \langle A \rangle$ is a monoid generated by a single primitive word.*

Lemma 2.4.18. *Let Y be an arbitrary generating set for $V_{2,1}$ and $y \in V_{2,1}$, then $y\langle A \rangle \setminus Y\langle A \rangle$ is finite.*

Proof. Note that if $y \in V_{2,1}$ then y belongs to the algebra generated by Y. Suppose that, when expressed in terms of the generators Y the λ-length of y is m, then we have $y\alpha_{i_1}...\alpha_{i_r} \in Y\langle A \rangle$ whenever $r \geq m$. That is, upon applications of $r \geq m$ of the unary operations of Ω to y we get an element which belongs to $Y\langle A \rangle$. Hence, the only elements of the set difference $y\langle A \rangle \setminus Y\langle A \rangle$ are those of the form $y\alpha_{i_1}...\alpha_{i_r}$ with $r < m$, and there are clearly only finitely many in number since we only have two choices for each α_{i_j}. □

The properties of bases of $V_{2,1}$ are now investigated, starting with a lemma from [Hig74].

Lemma 2.4.19. *[Hig74, Section 2, Lemma 2.4] Let X be an expansion of $\{x\}$. If U is a subset of $V_{2,1}$ contained in $X\langle A \rangle$, then the following are equivalent:*

1. *$U = X\langle A \rangle \cap Y\langle A \rangle$, for some arbitrary generating set Y of $V_{2,1}$,*
2. *U is A-closed and $X\langle A \rangle \setminus U$ is finite,*
3. *$U = Z\langle A \rangle$ for some expansion Z of X.*

Proof. Firstly, let $U = X\langle A \rangle \cap Y\langle A \rangle$. Since U is the intersection of A-closed sets, it is also A-closed. By lemma 2.4.18, $X\langle A \rangle \setminus Y\langle A \rangle$ is finite and therefore $X\langle A \rangle \setminus U$ is finite. So 1. implies 2.

Secondly, assume that U is A-closed and $X\langle A \rangle \setminus U$ is finite. We will prove 3. by induction on the size of $|X\langle A \rangle \setminus U|$. If $|X\langle A \rangle \setminus U| = 0$, then 3. holds with $Z = X$. Otherwise, $|X\langle A \rangle \setminus U| > 0$ and we choose an element $w \in X\langle A \rangle \setminus U$ of greatest length ($|w|$ is maximal). Then the set $U^* = U \cup \{w\}$ is A-closed and $|X\langle A \rangle \setminus U^*| = |X\langle A \rangle \setminus U| - 1$. By induction, there is an expansion Z^* of X such that $U^* = Z^*\langle A \rangle$. The element w belongs to Z^*, otherwise w would have the form $w = z\alpha_{i_1}...\alpha_{i_r}$, where

$z \in Z^*$ and $r > 0$, and hence $z \in U^* \setminus \{w\} = U$. However, U is A-closed and so this would imply that $w \in U$, a contradiction. If we take

$$Z = (Z^* \setminus \{w\}) \cup \{w\alpha_i | 1 \leq i \leq 2\},$$

then this is an expansion of $\{x\}$ and by the choice of w we have $w\alpha_i \in U$ for each i. Therefore $U = Z\langle A \rangle$.

Finally, if $U = Z\langle A \rangle$ for some expansion Z of X, then it is clear that $U = X\langle A \rangle \cap Y\langle A \rangle$, for some basis Y of $V_{2,1}$.

□

Definition 2.4.20. Let u, v be elements of $V_{2,1}$. Then, u is said to be a *proper initial segment of* v if $v = u\Gamma$ for some non-trivial $\Gamma \in \langle A \rangle$.

We will say u is an initial segment of v if $u = v$ or u is a proper initial segment of v.

Lemma 2.4.21. *[Hig74, Section 2, Lemma 2.5(i)-(iii)] Let X be a basis of $V_{2,1}$ and V a subset of $X\langle A \rangle$.*

1. *If X and V are finite, then V is contained in an expansion of X if and only if the following condition is satisfied:*

   (†) *no element of V is a proper initial segment of another.*

2. *If X and V are finite, then V is an expansion of X if and only if* (†) *is satisfied and for each $u \in X\langle A \rangle$ there exists $v \in V$ such that one of u, v is an initial segment of the other.*

3. *V is a set of free generators for the subalgebra it generates if and only if* (†) *is satisfied.*

Proof. 1. If V is contained in an expansion of X then (†) is satisfied.

Suppose V satisfies (†) and write

$$U = X\langle A \rangle \setminus \{\text{proper initial segments of elements of } V\}.$$

Then (†) implies that $V \subseteq U$. Also, U is A-closed and $X\langle A \rangle \setminus U$ consists of initial segments of the elements of the finite set V, so it is finite. Thus, by Lemma 2.4.19, there is an expansion Z of X such that $U = Z\langle A \rangle$. Therefore, $U \subseteq Z\langle A \rangle$, and this implies that $V \subseteq Z$ (for an element of $Z\langle A \rangle \setminus Z$ has a proper initial segment in $Z \subseteq U$ so it can not be in V by the definition of U). Hence, V is contained in an expansion of X.

2. If V is an expansion of X then $(\dagger)$ is satisfied and for each $u \in X\langle A\rangle$ there exists $v \in V$ such that one of u, v is an initial segment of the other.

   Suppose V satisfies $(\dagger)$ and for each $u \in X\langle A\rangle$ there exists $v \in V$ such that one of u, v is an initial segment of the other. By Part 1, V is contained in an expansion Z of X. If $V \neq Z$ then there is an element $z \in Z \setminus V$ and hence by the hypothesis there exists $v \in V$ such that one of v or z is an initial segment of the other. But no element of Z can be an initial segment of another, so this is a contradiction and hence $V = Z$.

3. If V is a set of free generators for the subalgebra it generates then $(\dagger)$ is satisfied.

   Suppose $(\dagger)$ is satisfied. If V is not a free generating set then the same is true of some finite subset V_0 and clearly $(\dagger)$ is also satisfied with V replaced by V_0. However, $V_0 \subseteq X_0\langle A\rangle$ for some finite subset X_0 of X. X_0 generates a free sub-Ω-algebra of $V_{2,1}$ and by [Hig74, Corollary 2, page 12] (since this is a $\mathcal{V}_2$-algebra) it follows that in fact X_0 generates an algebra isomorphic to $V_{2,1}$ and so contradicts Part 2.

□

The following corollary is an adaptation to [Hig74, Section 2, Corollary 1].

Corollary 2.4.22. *Any finite collection of bases $Y_1, ..., Y_n$ of $V_{2,1}$ has a unique minimal common expansion Z, which satisfies $Z\langle A\rangle = \cap_{i=1}^{n}(Y_i\langle A\rangle)$.*

Proof. For $n = 2$, let $U = Y_1\langle A\rangle \cap Y_2\langle A\rangle$. Then U is A-closed and by Lemma 2.4.19, $\{x\}\langle A\rangle \backslash U$ is finite. Hence $U = Z\langle A\rangle$, for some expansion Z of $\{x\}$. As $Z \subseteq Z\langle A\rangle \subseteq Y_i\langle A\rangle$, it follows from Lemma 2.4.21 part 2 that Z is an expansion of Y_i, $i = 1, 2$. Furthermore, if W is a common expansion of Y_1 and Y_2 then $W \subseteq U$, so $W \subseteq Z\langle A\rangle$, which implies that W is an expansion of Z.

Let $Z\langle A\rangle = \cap_{i=1}^{n-1}(Y_i\langle A\rangle)$ and $V = Z\langle A\rangle \cap Y_n\langle A\rangle$, where we assume inductively that Z is the unique minimal expansion of $Y_1, ..., Y_{n-1}$. From the previous paragraph there exists a unique minimal expansion W of Z and Y_n such that $W\langle A\rangle = V$. It follows that the result holds for $Y_1, ..., Y_n$ and hence by induction for all n. □

Example 2.4.23. Let $Y_1 = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2\alpha_2\}$ and $Y_2 = \{x\alpha_1\alpha_1, x\alpha_1\alpha_2, x\alpha_2\}$. Then, a common expansion of Y_1 and Y_2 is given by $Z = \{x\alpha_1\alpha_1, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2\alpha_2\}$.

It is easy to see that any other common expansion of Y_1 and Y_2 is also an expansion of Z.

If we have two bases Y and Z of $V_{2,1}$, what is the relationship between the two? The following lemma from Graham Higman gives some information about this.

Lemma 2.4.24. *[Hig74, Section 2, Lemma 2.5(iv)] Let X be a basis of $V_{2,1}$. Let Y and Z be d-fold expansions of X, for $d \geq 1$. If $Y \neq Z$ then some element of Y is a proper initial segment of an element of Z.*

Proof. We prove this by contradiction. If no element of Y is a proper initial segment of an element of Z *i.e.* there exists no $y \in Y$ such that there exists $\Gamma \in \langle A \rangle$ and $z \in Z$ with $y\Gamma = z$, then $Y \subseteq Z\langle A \rangle$. This implies that Y is an expansion of Z. However, Y and Z are both d-fold expansions of X and thus $Y = Z$. This competes the proof. □

2.5 The Higman-Thompson group $G_{2,1}$

We define the group we wish to study for the remainder of Part I of this thesis.

Definition 2.5.1. [Hig74] The *Higman-Thompson group* $G_{2,1}$ is the group of Ω-algebra automorphisms of $V_{2,1}$.

Remark 2.5.2. Let ψ be an automorphism of $V_{2,1}$ defined by the map $\psi : Y \to Z$, for Y, Z bases of $V_{2,1}$. Then, if we expand $y \in Y$ and form the basis $Y' = Y \setminus \{y\} \cup \{y\alpha_1, y\alpha_2\}$, then $y\alpha_i\psi = y\psi\alpha_i = z\alpha_i$ for $i = 1, 2$. Thus, if we expand the basis Y, then the automorphism ψ induces an expansion Z' of the basis Z such that $Y'\psi = Z'$.

Throughout this section, let $\mathbf{x}$ be a fixed expansion of $\{x\}$

Lemma 2.5.3. *[Hig74, Lemma 4.1] If $\{\psi_1, ..., \psi_k\}$ is a finite subset of $G_{2,1}$ then there is a unique minimal expansion Y of $\mathbf{x}$ such that $Y\psi_i \subseteq \mathbf{x}\langle A \rangle$, for $i = 1, ..., k$. That is, any other expansion of $\mathbf{x}$ with this property is an expansion of Y.*

Proof. [Hig74, Lemma 4.1]

For each i, $\mathbf{x}\psi_i^{-1}$ is a generating set for $V_{2,1}$, because $\mathbf{x}$ is a generating set and ψ_i is an automorphism (but $\mathbf{x}\psi_i^{-1} \notin \mathbf{x}\langle A \rangle$). Let $U_i = \mathbf{x}\langle A \rangle \cap \mathbf{x}\psi_i^{-1}\langle A \rangle$. Thus by Lemma 2.4.19 U_i is A-closed and there exists an expansion Y_i of $\mathbf{x}$ such that $U_i = Y_i\langle A \rangle$ (Y_i is also a basis of $V_{2,1}$ by Lemma 2.4.9). Now, Corollary 2.4.22 gives a unique minimal common expansion Y, of the Y_i's, and $Y\langle A \rangle = \cap_{i=1}^{k}(Y_i\langle A \rangle)$. Then, for all i, $Y \subseteq Y_i\langle A \rangle = U_i \subseteq \mathbf{x}\psi_i^{-1}\langle A \rangle$, so $Y\psi_i \subseteq \mathbf{x}\langle A \rangle$.

Let Z be an expansion of $\mathbf{x}$. If $Z\psi_i \subseteq \mathbf{x}\langle A \rangle$, for all i, then (by the definition of U_i) $Z \subseteq U_i = Y_i\langle A \rangle$, so $Z \subseteq \cap_{i=1}^{k}(Y_i\langle A \rangle) = Y\langle A \rangle$. Hence, from Lemma 2.4.19 and Corollary 2.4.22, Z is an expansion of Y. □

Remark 2.5.4. The above lemma gives a way of describing the elements of $G_{2,1}$ as bijections between expansions of $\{x\}$ of the same cardinality. Firstly, for the identity element this is clear, $1_{G_{2,1}} : \mathbf{x} \to \mathbf{x}$. For every element $\psi \in G_{2,1}$, by the lemma above, there is a unique minimal basis Y of $V_{2,1}$ such that $Y\psi = Z \subset \mathbf{x}\langle A \rangle$. Thus Z is also a

basis and $Z\psi^{-1} = Y$ (Z will be the unique minimal expansion corresponding to ψ^{-1}). Let $\psi : Y \to Z$ and $\varphi : U \to V$, with Y, Z, U and V all bases of $V_{2,1}$. Then we can define the product by finding the common expansion W for Z and U, which exists by Corollary 2.4.22, and expand Y and V according to the images $W\psi^{-1} = Y'$ and $W\varphi = V'$, noting that an expansion of an expansion of $\{x\}$ is an expansion of $\{x\}$. Then,

$$\psi\varphi : Y' \to V',$$

that is, $Y'\psi\varphi = W\varphi = V'$, and $\psi\varphi$ is an element of $G_{2,1}$. Associativity holds in a similar way.

Lemma 2.5.5. *Let X be a basis of $V_{2,1}$, let $u \in V_{2,1}$ and let d be a non-negative integer.*

1. *If $v \in V_{2,1}$ then $u = v$ if and only if $u\Gamma = v\Gamma$, for all $\Gamma \in \langle A \rangle$ of length d.*
2. *If S is a subalgebra of $V_{2,1}$ then $u \in S$ if and only if $u\Gamma \in S$, for all $\Gamma \in \langle A \rangle$ of length d.*

Proof. 1. If $u = v$ then $u\Gamma = v\Gamma$ for all $\Gamma \in \langle A \rangle$ of length d.

We shall show that given $d \geq 0$,

$$\text{if } u, v \in V_{2,1} \text{ and satisfy } u\Gamma = v\Gamma \text{ for all } \Gamma \in \langle A \rangle \text{ of length } d \text{ then } u = v. (\dagger\dagger)$$

If $d = 0$ this holds trivially. We will use induction on d. Assume that $d > 0$ and that for all d' such that $0 \leq d' < d$ $(\dagger\dagger)$ holds, with d' instead of d. Suppose then that $u, v \in V_{2,1}$ and $u\Gamma = v\Gamma$ for all Γ of length d. In this case we will show that for any $\Delta \in \langle A \rangle$ of length $d-1$ we have $u\Delta = v\Delta$. In fact, if Δ has length $d-1$ then $\Delta\alpha_i$ has length d, for $i = 1, 2$. Therefore, $u(\Delta\alpha_i) = v(\Delta\alpha_i)$ and we obtain $u\Delta = (u\Delta)\alpha_1(u\Delta)\alpha_2\lambda = (v\Delta)\alpha_1(v\Delta)\alpha_2\lambda = v\Delta$. This applies to all Δ of length $d-1$, as required. From the inductive hypothesis $u = v$.

2. If $u \in S$ then $u\Gamma \in S$ for all $\Gamma \in \langle A \rangle$ (and certainly for all Γ of length d).

We shall show that given $d \geq 0$,

$$\text{if } u \in V_{2,1} \text{ and satisfies } u\Gamma \in S \text{ for all } \Gamma \in \langle A \rangle \text{ of length } d \text{ then } u \in S. (\star)$$

If $d = 0$ this holds trivially. We will use induction on d. Assume that $d > 0$ and that for all d' such that $0 \leq d' < d$ $(\star)$ holds, with d' instead of d. Suppose then that $u \in V_{2,1}$ and $u\Gamma \in S$ for all Γ of length d. In this case we will show that for any $\Delta \in \langle A \rangle$ of length $d-1$ we have $u\Delta \in S$. In fact, if Δ has length $d-1$ then $\Delta\alpha_i$ has length d, for $i = 1, 2$. Therefore, $u(\Delta\alpha_i) \in S$ and we obtain

$u\Delta = (u\Delta)\alpha_1(u\Delta)\alpha_2\lambda \in S$. This applies to all Δ of length $d-1$, as required. From the inductive hypothesis $u \in S$.

□

Coming up is a series of subsections which discuss the work of [Hig74, Section 9]. This work will be needed in understanding the solution conjugacy problem.

2.5.1 Semi-normal forms

In [Hig74, Section 9], Higman picks an element ψ of $G_{2,1}$ and constructs a basis Y for $V_{2,1}$ in order to make the study of ψ easy (as he can then just examine the orbits of elements from Y).

Remark 2.5.6. In Matt Brin [Brin04] and Bleak et al [BGG11] revealing tree pairs divulge the dynamical information for a given element of $G_{2,1}$ acting on the Cantor set and this is similar to Higman's method.

The method is based on studying how ψ-orbits intersect the A-subalgebra $\mathbf{x}\langle A\rangle$ (for our fixed expansion $\mathbf{x}$ of $\{x\}$). Since ψ is an automorphism of $V_{2,1}$, we may have ψ-orbits which intersect the A-subalgebra $\mathbf{x}\langle A\rangle$ in one of four ways:

- the whole of the ψ-orbit is contained in $\mathbf{x}\langle A\rangle$ and is infinite;
- the whole of the ψ-orbit is contained in $\mathbf{x}\langle A\rangle$ and is finite;
- the ψ-orbit intersects $\mathbf{x}\langle A\rangle$ non-trivially, infinitely many times;
- the ψ-orbit intersects $\mathbf{x}\langle A\rangle$ non-trivially, only finitely many times.

We therefore can distinguish each ψ-orbit in the following way (according to its intersection with the A-subalgebra $\mathbf{x}\langle A\rangle$):

1. *Complete infinite orbits.* For any y in such an orbit, $y\psi^i$ belongs to $\mathbf{x}\langle A\rangle$ for all $i \in \mathbb{Z}$, and the elements $y\psi^i$ are all different.
2. *Complete finite orbits.* For any y in such an orbit, $y\psi^n = y$ for some positive integer n, and $y, y\psi, ..., y\psi^{n-1}$ all belong to $\mathbf{x}\langle A\rangle$.
3. *Right semi-infinite orbits.* For some y in the orbit, $y\psi^i$ belongs to $\mathbf{x}\langle A\rangle$ for all $i \geq 0$, but $y\psi^{-1}$ does not. The elements $y\psi^i$, $i \geq 0$, are then, of course, necessarily all different.
4. *Left semi-infinite orbits.* For some y in the orbit, $y\psi^{-i}$ belongs to $\mathbf{x}\langle A\rangle$ for all $i \geq 0$, but $y\psi$ does not. The elements $y\psi^{-i}$, $i \geq 0$, are then, of course, necessarily all different.

5. *Incomplete orbits.* For some y in the orbit and some non-negative integer n we have $y, y\psi, ..., y\psi^n$ belonging to $\mathbf{x}\langle A\rangle$ but $y\psi^{-1}$ and $y\psi^{n+1}$ do not.

Remark 2.5.7. Incomplete orbits will turn out to have finite intersection with $\mathbf{x}\langle A\rangle$ and it may be true that several incomplete orbits really belong to the same ψ-orbit in $V_{2,1}$.

We shall now clarify our terminology regarding the orbits of ψ in $V_{2,1}$ and the intersection of such orbits with $\mathbf{x}\langle A\rangle$ and summarise the above.

An *orbit* of ψ (in $V_{2,1}$) is a set $\{y\psi^n | n \in \mathbb{Z}\}$, for some fixed $y \in V_{2,1}$. The intersection of a given orbit of ψ (in $V_{2,1}$) with $\mathbf{x}\langle A\rangle$ might consist of infinitely many disjoint sequences $y_i, \ldots, y_i\psi^{n_i}$; or of infinitely many such things as well as either a left or right semi-infinite sequence of elements of $\mathbf{x}\langle A\rangle$; or of a left and a right semi-infinite sequence of elements of $\mathbf{x}\langle A\rangle$ as well as several of these disjoint finite sequences of elements of $\mathbf{x}\langle A\rangle$; or of finitely many disjoint sequences $y_i, \ldots, y_i\psi^{n_i}$ and either a left or right semi-infinite sequence (or neither).

Now let $y \in V_{2,1}$ and let $\psi \in G_{2,1}$. What Higman means by an "orbit of ψ in $\mathbf{x}\langle A\rangle$" is a maximal subsequence $\mathcal{O}$ of the sequence $y\psi^{i}{}_{i=-\infty}^{i=\infty}$ (that is of the orbit of y), such that all elements of $\mathcal{O}$ are in $\mathbf{x}\langle A\rangle$. It then follows that all such"orbits" are of types 1–5. We will refer to what Higman calls an "orbit of ψ in $\mathbf{x}\langle A\rangle$" as an $\mathbf{x}\langle A\rangle$-component of an orbit. From the definitions above, 1, 2, 3, 4, and 5 are then the possible types of $\mathbf{x}\langle A\rangle$-components of orbits.

When we talk about an "incomplete orbit" or a "semi-infinite orbit" we really mean an $\mathbf{x}\langle A\rangle$-component of an orbit.

Example 2.5.8. Let $X = \{x\}$ and,

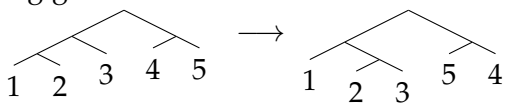
$$Y = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$$

and

$$Z = \{x\alpha_1^2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2^2, x\alpha_2\alpha_1\}.$$

Let ψ be the automorphism defined by $Y\psi = Z$, such that $y_i\psi = z_i$ for $i = 1, ..., 5$ with the ordering given above.

ψ :



We can see that $x\alpha_1^3$ is in a left semi-infinite orbit, $x\alpha_1\alpha_2$ is in a right semi-infinite orbit, $x\alpha_1^2\alpha_2$ is in a complete infinite orbit and finally $x\alpha_2\alpha_1, x\alpha_2^2$ are in the same complete finite orbit. (We defer an example of an incomplete finite orbit until later.)

We can now start to analyze an element ψ of the group $G_{2,1}$. By Lemma 2.5.3, for suitable d-fold expansions Y and Z of $\mathbf{x}$, we have $Y\psi = Z$ *i.e.* Y is the unique expansion given by Lemma 2.5.3 and Z the image of Y under ψ in $\mathbf{x}\langle A\rangle$.

Given that Z is a d-fold expansion of $\mathbf{x}$, $\mathbf{x}\langle A\rangle \setminus Z\langle A\rangle$ is finite. Similarly, it follows that $\mathbf{x}\langle A\rangle \setminus Y\langle A\rangle$ is finite.

As we have chosen Y to be the expansion given by Lemma 2.5.3, $Y\langle A\rangle = \mathbf{x}\langle A\rangle \cap \mathbf{x}\langle A\rangle\psi^{-1}$, and moreover ψ maps no proper contraction of Y into $\mathbf{x}\langle A\rangle$. Hence

$$Z\langle A\rangle = Y\langle A\rangle\psi = \mathbf{x}\langle A\rangle\psi \cap \mathbf{x}\langle A\rangle.$$

Thus, if $u \in \mathbf{x}\langle A\rangle \setminus Z\langle A\rangle$ then $u \notin \mathbf{x}\langle A\rangle\psi$, so $u\psi^{-1} \notin \mathbf{x}\langle A\rangle$ and hence u is an initial element either of an incomplete orbit or of a right semi-infinite orbit *i.e.* in an orbit of type (3) or (5). Similarly, if $v \in \mathbf{x}\langle A\rangle \setminus Y\langle A\rangle$ then $v \notin \mathbf{x}\langle A\rangle\psi^{-1}$, so $v\psi \notin \mathbf{x}\langle A\rangle$ and hence v is a terminal element either of an incomplete orbit or of a left semi-infinite orbit *i.e.* in an orbit of type (4) or (5).

If $\mathcal{O}$ is an orbit of type (3) or (5), then by definition there exists an element u, an initial element of $\mathcal{O}$. Therefore, $u\psi^{-1} \notin \mathbf{x}\langle A\rangle$ so $u \notin \mathbf{x}\langle A\rangle\psi$, and so $u \in \mathbf{x}\langle A\rangle \setminus Z\langle A\rangle$. Similarly, if $\mathcal{O}$ is an orbit of type (4) or (5), then by definition there exists an element v, which is a terminal element of $\mathcal{O}$. Therefore, $v\psi \notin \mathbf{x}\langle A\rangle$ so $v \notin \mathbf{x}\langle A\rangle\psi^{-1}$ and so $v \in \mathbf{x}\langle A\rangle \setminus Y\langle A\rangle$.

However, since ψ is an automorphism of $V_{2,1}$ with $Y\psi = Z$, then Y and Z are both d-fold expansions for some d, and so $|\mathbf{x}\langle A\rangle \setminus Z\langle A\rangle| = |\mathbf{x}\langle A\rangle \setminus Y\langle A\rangle|$.

Let u be an initial element of an incomplete orbit $\mathcal{O}$. By the above, $u \in \mathbf{x}\langle A\rangle \setminus Z\langle A\rangle$ and by definition of an incomplete orbit, there is some nonnegative integer n such that $u, u\psi, ..., u\psi^n$ all belong to $\mathbf{x}\langle A\rangle$ but $u\psi^{n+1}$ does not. Since $u\psi^{n+1}$ is a terminal element of the incomplete orbit $\mathcal{O}$, we have that $u\psi^{n+1} \in \mathbf{x}\langle A\rangle \setminus Y\langle A\rangle$. Therefore, the initial elements of incomplete orbits in $\mathbf{x}\langle A\rangle \setminus Z\langle A\rangle$ and terminal elements of incomplete orbits in $\mathbf{x}\langle A\rangle \setminus Y\langle A\rangle$ pair up.

Given that the initial and terminal elements of the incomplete finite orbits must be in one-to-one correspondence, all we are left with in $|\mathbf{x}\langle A\rangle \setminus Z\langle A\rangle|$ (respectively $|\mathbf{x}\langle A\rangle \setminus Y\langle A\rangle|$) are initial (respectively terminal) elements in right (respectively left) semi-infinite orbits, hence there are as many right semi-infinite obits as left semi-infinite orbits.

The above can now be summarized by the lemma below (which comes from Graham Higman) for a given element ψ of $G_{2,1}$.

Lemma 2.5.9. *[Hig74, Lemma 9.1] Let ψ be an element of $G_{2,1}$. Then there are only finitely many $\mathbf{x}\langle A\rangle$-components of orbits of ψ in $\mathbf{x}\langle A\rangle$ of type (3), (4) and (5) and there are as many of type (3) as of type (4).*

We define a particularly "good" type of expansion of X (a basis for $V_{2,1}$) for a given automorphism of $G_{2,1}$.

Definition 2.5.10. [Hig74, Section 9] An element ψ of $G_{2,1}$ is in *semi-normal form* with

respect to the basis Y if no elements of $Y\langle A\rangle$ are in incomplete finite ψ-orbits for ψ *i.e.* if $Y\psi \subseteq \mathbf{x}\langle A\rangle$ and no elements of Y are in orbits of type (5).

We now quote the following lemma from Higman.

Lemma 2.5.11. *[Hig74, Lemma 9.2] For an element ψ of $G_{2,1}$ there exists a basis with respect to which ψ is in semi-normal form.*

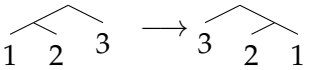
Proof. Let $\psi \in G_{2,1}$ and let Y be the minimal expansion associated to ψ (in the terminology suggested above). We prove the lemma by induction on the number of elements in $Y\langle A\rangle$ which belong to an incomplete orbit. Note first that from Lemma 2.5.9 it follows that there are only finitely many elements of $\mathbf{x}\langle A\rangle$, and hence also of $Y\langle A\rangle$, which belong to incomplete orbits.

If there are no such elements in $Y\langle A\rangle$ then we are done. Suppose then that there exists an element u in $Y\langle A\rangle$ which belongs in an incomplete orbit. Thus, there exist $y \in Y$ and $\Gamma \in \langle A\rangle$ such that $u = y\Gamma$ and some minimal $m, n \in \mathbb{N}_0$ such that $u\psi^{-(m+1)}, u\psi^{n+1} \notin \mathbf{x}\langle A\rangle$. It follows that $y\psi^{-(m+1)}, y\psi^{n+1} \notin \mathbf{x}\langle A\rangle$, so that y is also in an incomplete orbit. Let $Y' = Y\backslash\{y\}$ and let $Y'' = Y' \cup \{y\alpha_1, y\alpha_2\}$. Then Y'' is a basis for $V_{2,1}$, and $Y''\psi \subseteq \mathbf{x}\langle A\rangle$. Furthermore, the number of elements of $Y''\langle A\rangle$ in incomplete orbits is one less than the number in $Y\langle A\rangle$. Hence, by induction, there exists a basis with respect to which ψ is in semi-normal form. □

Example 2.5.12. Let $\mathbf{x} = \{x\}$ and let ψ be the automorphism of $G_{2,1}$ corresponding to the bijective map:

$$x\alpha_1^2\psi = x\alpha_2^2,\ x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1,\ x\alpha_2\psi = x\alpha_1.$$

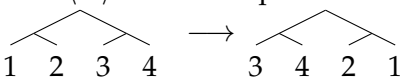
Then, $x\alpha_2$ is in an incomplete orbit. Firstly, $x\alpha_2\psi^{-1} \notin \mathbf{x}\langle A\rangle$ and secondly, $x\alpha_2\psi^2 \notin \mathbf{x}\langle A\rangle$.

ψ : 

However, if we choose to make a simple expansion at $x\alpha_2$, we notice that the bijective map now looks like this:

$$x\alpha_1^2\psi = x\alpha_2^2,\ x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1,\ x\alpha_2\alpha_1\psi = x\alpha_1^2, x\alpha_2^2 = x\alpha_1\alpha_2.$$

Hence, all elements of this new basis Y are in finite complete ψ-orbits. Therefore all elements of $Y\langle A\rangle$ are in complete finite orbits.

ψ : 

We give specific names to elements of a basis Y giving ψ in semi-normal form, based on the type of ψ-orbit the element is in. We give the following lemma without proof.

Lemma 2.5.13. *[Hig74, Lemma 9.3] Let ψ be an element of $G_{2,1}$ in semi-normal form with respect to the basis Y. Suppose that y is an element in Y, then one of the following holds,*

(A) There exists $\Gamma \in \langle A \rangle$ such that $y\Gamma$ is in a complete finite orbit. In this case y itself belongs to a complete finite orbit, which consists of elements of Y, and we say y is of type (A).

(B) There exist $\Gamma, \Delta \in \langle A \rangle$, with $\Gamma \neq \Delta$, such that $y\Gamma$ and $y\Delta$ belong to the same orbit. In this case there exists $\Lambda \in \langle A \rangle$, $n \in \mathbb{Z}$, $n \neq 0$, with $|n|$ minimal, such that $y\psi^n = y\Lambda$ and we say y is of type (B). If $n > 0$ then the orbit containing y is right semi-infinite; if $n < 0$ then the orbit containing y is left semi-infinite.

(C) y is not of type (A) or (B) above and there exists some $z \in Y$ of type (B) and non-trivial $\Delta \in \langle A \rangle$ such that $y\psi^i = z\Delta$. In this case the orbit containing y is infinite; and we say y is of type (C).

We will often refer to elements of type (A), (B) and (C). We now give the associated Γ for a type (B) element a name.

Definition 2.5.14. Let $u \in V_{2,1}$ and $\psi \in G_{2,1}$. If $u\psi^d \in u\langle A \rangle$ for some $d \in \mathbb{Z} \setminus \{0\}$ then u is a characteristic element for ψ.

If u is a characteristic element for ψ then the *characteristic* of u is the pair (m, Γ) such that $m \in \mathbb{Z} \setminus \{0\}$, $\Gamma \in \langle A \rangle$ with

- $u\Gamma^m = u\Gamma$ and
- for all n such that $0 < |n| < |m|$, $u\psi^n \notin u\langle A \rangle$.

In this case Γ is called the *characteristic multiplier* and m is the *characteristic power* for u, with respect to ψ. If Γ is non-trivial then it is said to be *proper* and we call u a *proper characteristic element*.

Remark 2.5.15. If u is a characteristic element then

1. (m, Γ) is uniquely determined and
2. if v is in the same orbit as u then v is a characteristic element with the same characteristic as u.

For 1. suppose that u is a characteristic element and with characteristic (m, Γ). If $u\psi^{m'} = u\Delta$ and for all n such that $0 < |n| \leq |m'|$ $u\psi^n \notin u\langle A \rangle$ then $|m'| \geq |m|$ by Definition 2.5.14 and so $m = \pm m'$. If $u\psi^{-m} = u\Delta$ then $u = u\psi^m\Delta = u\Gamma\Delta$, which can not happen.

For 2. let $v\psi^r = v\Gamma$. For all n such that $u\psi^n = u\Delta$, $\Delta \in \langle A \rangle$ we have,

$$v\psi^n = u\psi^r\psi^n = u\psi^n\psi^r = u\Delta\psi^r = u\psi^r\Delta = v\Delta.$$

Interchanging u and v we see also that whenever $v\psi^n = v\Delta$ then $u\psi^n = u\Delta$.

Given this remark we can make the following definition.

Definition 2.5.16. Let ψ be an element of $G_{2,1}$ and $\mathcal{O}$ a ψ-orbit containing a characteristic element u. Then we define the characteristic of $\mathcal{O}$ to be equal to the characteristic of u.

Example 2.5.17. From Example 2.5.8, the elements in the semi-infinite orbits $x\alpha_1^3$, $x\alpha_1\alpha_2$ are of type (B). In fact $x\alpha_1^3$ is a characteristic element of ψ^{-1} with $\Gamma_1 = \alpha_1$ and $x\alpha_1\alpha_2$ is a characteristic element of ψ with $\Gamma_2 = \alpha_2$.

Furthermore, the element $x\alpha_1^2\alpha_2$ is of type (C) and $x\alpha_2\alpha_1, x\alpha_2^2$ are elements of type (A).

We end this subsection with a result that allows us to determine if an element of $G_{2,1}$ is of infinite order.

Theorem 2.5.18. *[Hig74, Theorem 9.4] An element ψ of $G_{2,1}$ (given in semi-normal form with respect to Y) is of infinite order if and only if ψ^m has a proper characteristic element for some m. Moreover, if ψ is of infinite order then this proper characteristic element may be taken to belong to Y.*

Proof. [Hig74, Theorem 9.4] Let ψ be in semi-normal form with respect to the basis Y. If u is a characteristic element for ψ^m with proper multiplier Γ then $u\psi^m = u\Gamma$. Therefore,

$$u\psi^{mj} = u\psi^m\psi^{m(j-1)} = u\Gamma\psi^{m(j-1)} = u\Gamma\psi^m\psi^{m(j-2)} = u\psi^m\Gamma\psi^{m(j-2)} = u\Gamma^2\psi^{m(j-2)} = \ldots = u\Gamma^j,$$

for $j \in \mathbb{N}$. Since Γ is a proper multiplier, the elements $u\Gamma^j$ are all different for $j \in \mathbb{N}$, so ψ has infinite order.

Conversely, if no ψ^m with $m \in \mathbb{Z}$ has a proper characteristic element then Y has no elements of type (B) nor type (C). Thus all elements of Y are of type (A), as ψ is in semi-normal form with respect to the basis Y. Whence ψ is a permutation of Y and has finite order. □

Lemma 2.5.19. *Let ψ be in semi-normal form with respect to a basis Y and let $u \in V_{2,1}$. If u has characteristic (m, Γ) then the orbit of u is semi-infinite (right semi-infinite if $m > 0$ and left semi-infinite if $m < 0$) and contains an element $y\Gamma_1$, where $y \in Y$, y is of type (B) and y has characteristic $(m, \Gamma_1\Gamma_0)$, where $\Gamma = \Gamma_0\Gamma_1$ and Γ_0 is non-trivial. (It is possible that Γ_1 is trivial.)*

Proof. Let $\mathcal{O}$ be the orbit of u. Note that if $v \in \mathcal{O}$ then $v = u\psi^k$, for some $k \in \mathbb{Z}$, so $v\psi^m = u\psi^{m+k} = u\Gamma\psi^k = u\psi^k\Gamma = v\Gamma$, and it follows that every element v has characteristic (m, Γ). For some $q \geq 0$ we have $u\Gamma^q \in Y\langle A\rangle$, so $u\psi^{mq} = u\Gamma^q \in Y\langle A\rangle$.

Hence we may assume that $u \in Y\langle A\rangle$. Let $u = y\Lambda$, where $y \in Y$ and $\Lambda \in \langle A\rangle$. We assume first that $m > 0$. If $\mathcal{O}$ is not right semi-infinite then, as ψ is in semi-normal form with respect to Y, we have $u\psi^{-k} \in \mathcal{O}$, for all $k \geq 0$. Let $\Lambda = \Lambda_0\Gamma^j$, where Λ_0 has no terminal segment equal to Γ. Then $u\psi^{-m(j+1)} \in \mathcal{O}$, so for some $z \in Y$ and $\Xi \in \langle A\rangle$, $u\psi^{-m(j+1)} = z\Xi$ and so

$$z\Xi\Gamma^{j+1} = z\Xi\psi^{m(j+1)} = u = y\Lambda_0\Gamma^j,$$

so $z = y$ and $\Xi\Gamma = \Lambda_0$, a contradiction. Hence $\mathcal{O}$ is right semi-infinite. Moreover, we may assume that Λ has no terminal segment equal to Γ.

Now $u = y\Lambda \in \mathcal{O}$ and $y\Lambda\psi^m = y\Lambda\Gamma$ so, by Lemma 2.5.13, y is of type (B). Suppose y has characteristic (n, Ω). If the orbit of y is left semi-infinite then $y\Lambda\psi^{-k} \in Y\langle A\rangle$, for all $k \geq 0$, so $\mathcal{O}$ is not right semi-infinite. Hence y is in a right semi-infinite orbit and $n > 0$. If $\Lambda = \Omega^j\Lambda_1$ then $y\Lambda_1\psi^{nj} = y\Omega^j\Lambda_1 = u$, so we may assume that Λ has no initial segment equal to Ω. Suppose that $0 < n < m$ and write $m = np + r$, where $0 \leq r < n$. Then $y\Lambda\psi^{np} = y\Omega^p\Lambda$ and $y\Omega^p\Lambda\psi^r = y\Lambda\psi^{np+r} = y\Lambda\psi^m = y\Lambda\Gamma$. However, as y is in a right semi-infinite orbit, $y\psi^r = z\Xi$, for some $z \in Y$ and $\Xi \in \langle A\rangle$. Thus $y\Lambda\Gamma = y\Omega^p\Lambda\psi^r = y\psi^r\Omega^p\Lambda = z\Xi\Omega^p\Lambda$, which implies that $z = y$ and $\Lambda\Gamma = \Xi\Omega^p\Lambda$. Now, as $y\psi^r = y\Xi$, with $0 \leq r < n$, and y has characteristic (n, Ω), it must be that $r = 0$ and $\Xi = 1$. We have now $\Lambda\Gamma = \Omega^p\Lambda$ and, as Λ has no terminal segment equal to Γ and no initial segment equal to Ω, consequently $\Gamma = \Gamma_0\Lambda$ and $\Omega = \Lambda\Omega_1$. However this means that $y\Lambda\psi^n = y\Omega\Lambda = y\Lambda\Omega_1\Lambda$, and as $u = y\Lambda$ has characteristic power m, we infer that $n \geq m$, a contradiction.

Hence $0 < m \leq n$. Now $y\psi^m = y_1\Delta$, $y_1 \in Y$, $\Delta \in \langle A\rangle$, and so $y\Lambda\Gamma = y\Lambda\psi^m = y_1\Delta\Lambda$. Hence $y = y_1$ and $\Lambda\Gamma = \Delta\Lambda$. As Λ has no terminal segment equal to Γ this implies that $\Gamma = \Gamma_0\Lambda$ so $y\Lambda\Gamma_0\Lambda = y\Delta\Lambda$, from which it follows that $y\Lambda\Gamma_0 = y\Delta = y\psi^m$, so $m \geq n$. Hence $m = n$ and, setting $\Lambda = \Gamma_1$, the proof is complete, in the case $m > 0$.

In the case when $m < 0$ the result follows from the above on replacing ψ by ψ^{-1}. □

Lemma 2.5.20. *Let $\theta \in G_{2,1}$ and $u \in V_{2,1}$ such that $u\theta^n = u\Delta$, where $\Delta \neq 1$. Then u has characteristic (m, Γ) with respect to θ, where $n = mq$ and $\Delta = \Gamma^q$, for some positive integer q.*

Proof. Let θ be in semi-normal form with respect to X. Suppose first that $n > 0$. Then the ($X\langle A\rangle$-component of the) orbit $\mathcal{O}$ of u is right semi-infinite, and its elements have characteristic (m, Γ) with respect to θ, for some $m > 0$ and $\Gamma \neq 1$. Then $n \geq m$, so we may write $n = mq + s$, where $0 \leq s < m$ and $q \geq 0$. Thus $v\Delta = v\theta^n = v\theta^{mq+s} = v\Gamma^q\theta^s$, for all $v \in \mathcal{O}$. Choose $v \in \mathcal{O} \cap X\langle A\rangle$ (by choosing $v = u\Delta^{nk}$ for sufficiently large k).

Then $v = y\Lambda$, for some $y \in X$ and $\Lambda \in \langle A \rangle$, and y belongs to a right semi-infinite orbit of θ, as v does. Hence $y\theta^s = y'\Lambda'$, for some $y' \in X$, $\Lambda' \in \langle A \rangle$, and $y\Lambda\Delta = v\Gamma^q\theta^s = y'\Lambda'\Gamma^q$, so $y = y'$ and $y\theta^s = y\Lambda'$; so $v\theta^s = y\Lambda\theta^s = y\Lambda'\Lambda$. By minimality of m, we have $s = 0$, so $n = mq$. Moreover $y\Lambda\Delta = v\Delta = v\theta^n = v\theta^{mq} = v\Gamma^q = y\Lambda\Gamma^q$, so $\Lambda\Delta = \Lambda\Gamma^q$, from which $\Delta = \Gamma^q$, as required.

If $n < 0$ then let $\psi = \theta^{-1}$. We have $u\psi^{-n} = u\Delta$, so from the previous part of the proof, u has characteristic (m, Γ), with respect to ψ, where $-n = mq$, $q > 0$, and $\Delta = \Gamma^q$. If follows that u has characteristic $(-m, \Gamma)$, with respect to θ, and $-m = nq$, completing the proof. □

2.5.2 Quasi-normal forms

A stronger definition than semi-normal form was introduced in [Hig74, Section 9].

Definition 2.5.21. [Hig74, Section 9] An element ψ of $G_{2,1}$ is in *quasi-normal* form with respect to the basis Y if it is in semi-normal form with respect to Y, but not with respect to any proper contraction of Y.

It follows from Lemma 2.5.3 that for $\psi \in G_{2,1}$ there exists a basis Y with respect to which ψ is in quasi-normal form.

Once we have ψ in quasi-normal form we have the following lemma from Graham Higman (given here without proof).

Lemma 2.5.22. *[Hig74, Lemma 9.6] If ψ is in quasi-normal form with respect to Y, and if $v = u\psi^m$, where $m > 0$ and $u, v \in Y\langle A \rangle$, then $u\psi^i$ belongs to $Y\langle A \rangle$, for $i = 1, ..., m-1$.*

Lemma 2.5.23. *Let ϕ be in quasi-normal form with respect to Y and let $y \in Y$ be of type (B). Suppose that y has characteristic (m, Γ). Then there exist $\Gamma_i \in \langle A \rangle$ and $y_i \in Y$, $1 \leq |i| \leq |m|$, such that $y = y_m$; if $i \neq j$ then $y_i \neq y_j$; $\Gamma = \Gamma_m \cdots \Gamma_1$ if $m > 0$ and $\Gamma = \Gamma_m \cdots \Gamma_{-1}$ if $m < 0$; and*

$$y\phi^i = \begin{cases} y_i\Gamma_i \cdots \Gamma_1, & \text{for } 1 \leq i \leq m, \text{ if } m > 0 \\ y_i\Gamma_i \cdots \Gamma_{-1}, & \text{for } -1 \geq i \geq m, \text{ if } m < 0 \end{cases}.$$

Moreover, setting $\varepsilon = m/|m|$, y_i has characteristic multiplier $\Gamma_i' = \Gamma_i \cdots \Gamma_\varepsilon \Gamma_m \cdots \Gamma_{i+\varepsilon}$, and $y_i\phi^m = y_i\Gamma_i'$, for $1 \leq |i| \leq |m| - 1$.

Remark 2.5.24. The characteristic multiplier of $y_i\Gamma_i \cdots \Gamma_\varepsilon$ is Γ, for all i. However, the characteristic multipliers of the y_i themselves may not equal to Γ.

Proof. Assume $m > 0$, so the orbit of y is right semi-infinite. The proof in the other case is similar. Since ϕ is in quasi-normal form with respect to Y and y and $y\phi^m \in Y\langle A \rangle$, from Lemma 2.5.22 we have $y\phi^i \in Y\langle A \rangle$, for $1 \leq i \leq m-1$. Thus there exist

$y_i \in Y$ and $\Phi_i \in \langle A \rangle$ such that $y\phi^j = y_i\Phi_i$, for $1 \leq i \leq m-1$. Set $y_m = y$ and $\Phi_m = \Gamma$, and the latter holds for $1 \leq i \leq m$.

As $y_i\Phi_i\phi^m = y\phi^{m+i} = y\Gamma\phi^i = y_i\Phi_i\Gamma$, both $y_i\Phi_i$ and $y_i\Phi_i\Gamma$ belong to the same orbit of y and Lemma 2.5.13 (B) implies that for some $n_i \neq 0$ we have $y_i\phi^{n_i} = y_i\Delta_i$, for some $\Delta_i \neq 1$. If $n_i < 0$ then it follows that $y_i\phi^j \in Y\langle A \rangle$, for all $j \leq 0$, so $y\phi^{i+j} = y_i\Phi_i\phi^j \in Y\langle A \rangle$, for all $j \leq 0$, which is impossible, as the orbit of y is right semi-infinite. Hence $n_i > 0$, and (using Lemma 2.5.22) in particular $y_i\phi = z_i\Gamma_{i+1}$, for some $z_i \in Y$ and $\Gamma_{i+1} \in \langle A \rangle$.

Set $\Gamma_1 = \Phi_1$. Then $y\phi = y_1\Gamma_1$. Assume inductively that for $1 \leq k \leq i-1 < m$ we have $y\phi^k = y_k\Gamma_k \cdots \Gamma_1$. Then $y\phi^i = y\phi^{i-1}\phi = y_{i-1}\Gamma_{i-1} \cdots \Gamma_1\phi = y_{i-1}\phi\Gamma_{i-1} \cdots \Gamma_1 = z_{i-1}\Gamma_i\Gamma_{i-1} \cdots \Gamma_1$. Hence $y_i\Phi_i = y\phi^i = z_{i-1}\Gamma_i \cdots \Gamma_1$, so $z_{i-1} = y_i$ and $\Phi_i = \Gamma_i \cdots \Gamma_1$. By induction $y\phi^i = y_i\Gamma_i \cdots \Gamma_1$, for $i = 1, \ldots, m$. In particular, $y\phi^m = y_m\Gamma_m \cdots \Gamma_1$ and as $y_m = y$ we have $\Gamma = \Gamma_m \cdots \Gamma_1$.

From the above we have $y_i\phi = y_{i+1}\Gamma_{i+1}$, so

$$y_i\phi^m = y_{i+1}\Gamma_{i+1}\phi^{m-1} = \ldots = y_m\Gamma_m \cdots \Gamma_{i+1}\phi^i = \ldots = y_i\Gamma_i \cdots \Gamma_1\Gamma_m \cdots \Gamma_{i+1}.$$

Finally, if $1 \leq i < j \leq m$ and $y_i = y_j$, then $y_i\phi = y_j\phi$ so $y_{i+1}\Gamma_{i+1} = y_{j+1}\Gamma_{j+1}$, which implies that $y_{i+1} = y_{j+1}$ and $\Gamma_{i+1} = \Gamma_{j+1}$. Repeating this argument we obtain eventually $y_{m-j+i} = y_m = y$, and so $y\phi^{m-j+i} = y\Gamma_{m-j+i} \cdots \Gamma_1$, with $m - j + i < m$, a contradiction. Hence the y_i are all distinct and the proof is complete. □

One of the most useful lemmas of [Hig74] with regard to the ψ-orbits of elements of $V_{2,1}$ is given below, with proof. In the cases of interest when we are computing with elements in $G_{2,1}$ we assume the automorphism is given by a map between two bases.

Lemma 2.5.25. *[Hig74, Lemma 9.7] Given an element $\psi \in G_{2,1}$ there exists a unique basis Y_ψ with respect to which ψ is in quasi-normal form. Moreover, (i) we can effectively construct the basis Y_ψ and (ii) for $u, v \in V_{2,1}$ we can effectively decide whether or not u, v are in the same orbit of ψ, and if so, find the integers m for which $u\psi^m = v$.*

Proof. [Hig74, Lemma 9.7] For part (i), we shall start with an arbitrary basis Y and modify it until we have ψ given in semi-normal form with respect to a basis $\widehat{Y}$ such that no contraction of the basis $\widehat{Y}$ gives ψ in semi-normal form.

Suppose ψ is given by a bijection between bases Y and Y'. First we construct such a $\widehat{Y}$. For each $y \in Y$ we list elements of the orbit with respect to $\langle \psi \rangle$,

$$\ldots, y\psi^{-3}, y\psi^{-2}, y\psi^{-1}, y, y\psi, y\psi^2, y\psi^3, \ldots .$$

We begin with y go forward in the sequence to $y\psi^i$ for $i > 1$ until we reach for $m \geq 0$

such that,

(1F) either $y\psi^m \in Y\langle A\rangle$ with $y\psi^{m+1} \notin Y\langle A\rangle$ or,

(2F) for some l with $0 \leq l < m$ and for some $\hat{y} \in Y$ and $\Gamma, \Delta \in \langle A\rangle$, $y\phi^l = \hat{y}\Gamma$ and $y\phi^m = \hat{y}\Delta$.

Similarly, we go backwards in the sequence from y until we reach for $n \geq 0$ such that,

(1B) either $y\psi^{-n} \in Y\langle A\rangle$ with $y\psi^{-(n+1)} \notin Y\langle A\rangle$ or,

(2B) for some l with $0 \leq l < -n$ and for some $\hat{y} \in Y$ and $\Gamma, \Delta \in \langle A\rangle$, $y\phi^l = \hat{y}\Gamma$ and $y\phi^{-n} = \hat{y}\Delta$.

Given $y \in Y$, the forward part of the process above produces a sequence of elements of $Y\langle A\rangle$, until it halts. As Y is finite it therefore always halts. The backward part of the process above always halts for the same reason.

If some y satisfies **(1F)** and **(1B)**, then ψ was not in semi-normal form with respect to Y. Therefore, we expand Y at the element y and start again. If no $y \in Y$ satisfies **(1F)** and **(1B)**, then ψ is in semi-normal form with respect to Y by Lemma 2.5.11 and its proof..

We can now assume ψ is in semi-normal form with respect to Y. We can thus test all the contractions of the basis Y to find a basis with respect to which ψ is in a quasi-normal form.

For uniqueness, we will argue by contradiction. Let ψ be in quasi-normal form with respect to Y_1 and Y_2, with $Y_1 \neq Y_2$. By Lemma 2.5.3, there exists a unique minimal expansion Y such that $Y\psi \subseteq \mathbf{x}\langle A\rangle$ and any other basis Z, with the property $Z\psi \subseteq \mathbf{x}\langle A\rangle$, is an expansion of Y. Since ψ is in quasi-normal form with respect to Y_1 and Y_2 we have $Y_1 \neq Y_2$, $Y_i\psi \subseteq \mathbf{x}\langle A\rangle$ for $i = 1, 2$. Therefore, Y_1 and Y_2 are expansions of Y.

Since $Y_1 \neq Y_2$ and Y_1, Y_2 are expansions of Y, (without loss of generality) there exists a contraction of the basis Y_1 which gives an element y in Y_2. However, ψ is in semi-normal form with respect to Y_2. Thus, we could have contracted Y_1 to give ψ in semi-normal form and hence ψ was not in quasi-normal form with respect to Y_1 (because Y_1 was not a minimal expansion of $\{x\}$ giving ψ in semi-normal form). Therefore, the expansion of $\{x\}$ giving ψ in quasi-normal form is unique.

For part (ii), we may assume, by part (i), that we have ψ in quasi-normal form with respect to a basis Y. If the orbit of u is finite we can list all elements in the ψ-orbit of u and check to see if v appears in the list. Assume u is in an infinite orbit. Moreover, for a fixed integer $s \geq 0$ we have $u\psi^m = v$ if and only if

$$(u\Gamma)\psi^m = u\psi^m\Gamma = v\Gamma$$

for all $\Gamma \in \langle A \rangle$ of length s (using Lemma 2.5.5). Now, suppose that we have an algorithm $\mathcal{A}$ to decide whether $v' = u'\psi^m$, for some m, for elements u', v' of $Y\langle A \rangle$ (and to return m, if so). Then if u, v are arbitrary elements of $V_{2,1}$ we may choose s such that $u\Gamma$ and $v\Gamma$ belong to $Y\langle A \rangle$, for all $\Gamma \in \langle A \rangle$ of length s, and input all these elements to the algorithm $\mathcal{A}$ in turn. In the light of the previous remark, this allows us to determine whether or not u and v belong to the same orbit of ψ (and to return an appropriate m, if so). Hence we may assume $u, v \in Y\langle A \rangle$ and, by Lemma 2.5.22, as u and v belong to the same orbit of ψ in $V_{2,1}$, they belong to the same $Y\langle A \rangle$-component of an orbit of ψ.

As $u \in Y\langle A \rangle$, we have $u = y\Lambda$, where $y \in Y$ and $\Lambda \in \langle A \rangle$. We now run the process of part (i) on y. If the process halts with $y\psi^m = y$, for some m then we may list the elements $u\psi^i = y\psi^i\Lambda$, $i = 0, \ldots, m-1$, of the orbit of u. In this case v is in the same orbit as u if and only if it appears in the list, so we are done. Otherwise the process halts at (1F) and (2B), at (2F) and (1B) or at (2F) and (2B). In all cases we obtain $\widetilde{y} \in Y$ such that, for some $k \neq l$ and $\Lambda_1 \neq \Lambda_2 \in \langle A \rangle$, we have $y\phi^k = \widetilde{y}\Lambda_1$ and $y\phi^l = \widetilde{y}\Lambda_2$. It follows from Lemma 2.5.13 that $\widetilde{y}$ is of type (B). As $u\phi^k = y\Lambda\phi^k = \widetilde{y}\Lambda_1\Lambda$ we may replace $u = y\Lambda$ with $\widetilde{u} = \widetilde{y}\Lambda_1\Lambda$. Therefore we now assume that $u = y\Lambda$, where y is of type (B). Now, when we run the process of part (i) on y it halts at (2F) and (1B) or at (1F) and (2B). Suppose first the forward part halts at (2F). Then y is in a right semi-infinite orbit and there is a minimal positive integer m such that $y\psi^m = y\Gamma$, with $\Gamma \neq 1$.

Thus we have $u = y\Lambda$, where $y \in Y$ and $y\psi^m = y\Gamma$, with $m > 0$ and $\Gamma \neq 1$. If $\Lambda = \Gamma^i\Lambda_0$, where Λ_0 has no initial segment Γ, and we set $u_0 = y\Lambda_0$ then,

$$u_0\psi^{mi} = y\Lambda_0\psi^{mi} = y\psi^{mi}\Lambda_0 = y\Gamma^i\Lambda_0 = y\Lambda = u,$$

so u_0 is in the same orbit of $\langle \psi \rangle$ as u. Hence we may replace $u = y\Lambda$ by $u_0 = y\Lambda_0$. Once we have done this we may suppose Λ has no initial segment equal to the characteristic multiplier Γ of y.

From Lemma 2.5.23 above there exist $\Gamma_i \in \langle A \rangle$ and distinct $y_i \in Y$, for $i = 1, \ldots, m$, with $y = y_m$ and $\Gamma = \Gamma_m \cdots \Gamma_1$, such that, setting $\Delta_i = \Gamma_i \cdots \Gamma_1\Gamma_m \cdots \Gamma_{i+1}$ and $\Gamma'_i = \Gamma_i \cdots \Gamma_1$ (and $\Gamma'_0 = 1$), we have $y\psi^i = y_i\Gamma'_i$ and y_i has characteristic multiplier Δ_i, $i = 1, \ldots m$. Thus the $Y\langle A \rangle$-component of the orbit of y consists of the elements $y\psi^{mq+i} = y_i\Delta_i^q\Gamma'_i$, with $q \geq 0$, and finitely many elements $y\psi^{-j}$, where $j < 0$.

Next we run the process of (i) on u instead of y. As y is in a right semi-infinite orbit the forward part of the process halts at (2F). As the y_i's are distinct we obtain a list of elements of the orbit of u of the form

$$z_r\Phi_r, \cdots, z_1\Phi_1, u = y\Lambda, y_1\Gamma'_1\Lambda, \ldots, y_{m-1}\Gamma'_{m-1}\Lambda, y\Gamma\Lambda, \tag{2.8}$$

where $z_j \in Y$, $\Phi_j \in \langle A \rangle$, $z_j\Phi_j = u\psi^{-j}$, for $1 \leq j \leq r$ for some $r \geq 0$. If the backward part of the process halts at (1B) then $u\psi^{-r-1} \notin Y\langle A \rangle$. On the other hand, if the backward part of the process stops at (2B) then, for some s with $0 \leq s \leq r$, we have $z_r = z_s$ (and r is minimal with this property).

As $v \in Y\langle A \rangle$ we also have $z \in Y$ and Δ in $\langle A \rangle$ such that $v = z\Delta$. If z is in a finite orbit then v cannot belong to the same orbit as u, so we assume z is in an infinite $Y\langle A \rangle$-orbit. As in the case of u, we may adjust v so that z is of type (B). As before we find a characteristic multiplier Φ for z and, replacing Δ with a shorter element if necessary, we may assume that Δ has no initial segment equal to Φ.

Suppose first that the backward part of the enumeration of the orbit of u halts at (1B). In this case, the orbit of u has initial element $z_r\Phi_r$. If $v = u\psi^d$ then either $d < 0$ and $v = z_d\Phi_d$, with $1 \leq d \leq r$, or $d \geq 0$ and $v = y_i\Delta_i^q\Gamma_i'\Lambda$, for some $q \geq 0$. If the latter occurs, then $z = y_i$ and by our assumption on v we have $q = 0$, so $v = y_i\Gamma_i'\Lambda$. In both cases v appears on the list (2.8). Otherwise u and v do not belong to the same orbit.

Now suppose that the backward part of the enumeration of the orbit of u halts at steps (2B). Then u is in a complete infinite orbit and, for some s with $0 \leq s \leq r$, we have $z_r = z_s$. It follows that z_s is of type (B) and in a left semi-infinite orbit. As before, if $v = u\psi^d$ with $d \geq 0$ then $v = y_i\Gamma_i'\Lambda$, for some i with $0 \leq i \leq m-1$, so appears in the list (2.8). Now, if $v = u\psi^d$ with $d < 0$, then either $v = z_j\Phi_j$ with $1 \leq j \leq s$, or v lies to the left of $z_s\Phi_s$, in the orbit of u. However, arguing as in the first case, using Lemma 2.5.23, with z_s instead of y, we see that elements in the orbit of u to the left of $z_s\Phi_s$ have the form $z_j\Theta_j^p\Phi_j$, where $s \leq j < r$, $p \geq 0$, Θ_j is the characteristic multiplier of z_j and $z_j\psi^{r-s} = z_j\Theta_j$. Suppose then that $v = z_j\Theta_j^p\Phi_j$, for some such j and p. Writing $\Phi_j = \Theta_j^q\Phi_j'$, where Φ_j' has no initial segment equal to Θ_j, we have $z\Delta = v = z_j\Theta_j^{p+a}\Phi_j'$. Thus $z = z_j$ and the condition on Δ implies that $p + a = 0$. Therefore $\Phi_j = \Phi_j'$ and $v = z_j\Phi_j$, which belongs to the list (2.8).

Therefore, in the case where y is in a right semi-infinite orbit we have v in the orbit of u if and only if v lies on the list (2.8); and we may compute m such that $u\psi^m = v$, if this is the case. Finally, if the enumeration of the orbit of y halts at steps (1F) and (2B) then the process is essentially the same, except that we deal with a left, rather than a right, semi-infinite orbit of y. □

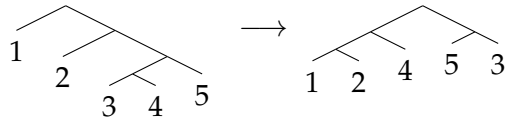
Example 2.5.26. Let φ be in quasi-normal form with respect to the basis

$$Y = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1^2, x\alpha_2^2\alpha_1\alpha_2, x\alpha_2^3\}$$

and defined by the bijection with the basis

$$W = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$$

given by $x\alpha_1\varphi = x\alpha_1^3$, $x\alpha_2\alpha_1\varphi = x\alpha_1^2\alpha_2$, $x\alpha_2^2\alpha_1^2\varphi = x\alpha_2^2$, $x\alpha_2^2\alpha_1\alpha_2\varphi = x\alpha_1\alpha_2$, $x\alpha_2^3\varphi = x\alpha_2\alpha_1$.

φ : 

We would like to decide if the elements $v_1 = x\alpha_1\alpha_2$ and $v_2 = x\alpha_1^2\alpha_2$ are in the orbit of $u = x\alpha_2^2\alpha_1^2\alpha_2$. As ψ is in quasi-normal form and u, v_1, v_2 are in $Y\langle A\rangle$ we begin by rewriting u as $y\Lambda$ so that $y \in Y$ and $\Lambda \in \langle A\rangle$. That is,

$$u = x\alpha_2^2\alpha_1^2\alpha_2 = (x\alpha_2^2\alpha_1^2)\alpha_2 = y_3\alpha_2,$$

where $y_3 = x\alpha_2^2\alpha_1^2 \in Y$ (the third element in the basis).

We now, for some k, find $\widetilde{y}$ an element of type (B) such that $u\varphi^k = \widetilde{y}\Lambda_1$. From the above, we can choose $\widetilde{y} = y_3 = x\alpha_2^2\alpha_1^2$ and so $k = 0$ and $\Lambda_1 = \Lambda$. The characteristic multiplier for $\widetilde{y}$ is α_1^2 and $\Lambda = \alpha_2$ has no initial segment equal to α_1^2 so we can take $u_0 = u = x\alpha_2^2\alpha_1^2\alpha_2$. We now look at the orbit of u,

	$u\varphi^{-1}$,	u,	$u\varphi$,	$u\varphi^2$,	$u\varphi^3$,	$u\varphi^4$,	
	$x\alpha_2^2\alpha_1^4\alpha_2$,	$x\alpha_2^2\alpha_1^2\alpha_2$,	$x\alpha_2^3$,	$x\alpha_2\alpha_1$,	$x\alpha_1^2\alpha_2$,	$x\alpha_1^4\alpha_2$,	
STOP 2B	$y_3\alpha_1^2\alpha_2$,	$y_3\alpha_2$,	y_5,	y_2,	$y_1\alpha_1\alpha_2$,	$y_1\alpha_1^3\alpha_2$,	STOP 2F

For $v_1 = x\alpha_1\alpha_2$, we can write $v = z\Delta$ with z of type (B). Here, $z = y_1 = x\alpha_1$ and $\Delta = \alpha_2$. Since Δ has no initial segment in common with the characteristic multiplier α_1^2 for z, we can take $v_0 = v_1$. We can now check the list above and see that v_0 does not appear in the list and so v is not in the same orbit of u.

For $v_2 = x\alpha_1^2\alpha_2$, we can write $v = z\Delta$ with z of type (B) (we see immediately that $u\varphi^3 = v$ but here we will follow the algorithm). Here, $z = y_1 = x\alpha_1$ and $\Delta = \alpha_1\alpha_2$. Since Δ has no initial segment in common with the characteristic multiplier α_1^2 for z, we can take $v_0 = v_2$. We can now check the list above and see that v_0 does appear in the list and in fact $u\varphi^3 = v$.

Chapter 3

The conjugacy and power conjugacy problems in $G_{2,1}$

In this chapter we examine the conjugacy and power conjugacy problems for the Higman-Thompson group $G_{2,1}$.

3.1 Higman's ψ-invariant subalgebras V_P and V_{RI}

Let ψ be an element of $G_{2,1}$. Higman defined two subalgebras of $V_{2,1}$, determined by ψ; namely

- the subalgebra $V_{P,\psi}$ generated by the set of elements of $V_{2,1}$ which belong to finite orbits of ψ and
- the subalgebra $V_{RI,\psi}$ generated by the set of elements of $V_{2,1}$ which have proper characteristic multipliers (that is elements u such that $u\psi^m = u\Gamma$, for some $m \in \mathbb{Z}$ and some $\Gamma \neq 1$).

Where there is no ambiguity, we will write V_P for $V_{P,\psi}$ and V_{RI} for $V_{RI,\psi}$. If φ is any element of $G_{2,1}$ then $\varphi|_{V_{P,\varphi}}$ and $\varphi|_{V_{RI,\varphi}}$ are isomorphisms between subalgebras of $V_{2,1}$. We write $\varphi_P = \varphi|_{V_{P,\varphi}}$ and $\varphi_{RI} = \varphi|_{V_{RI,\varphi}}$.

Now suppose that ψ is in semi-normal form with respect to a basis Y. We first partition Y into the following disjoint sets,

$$Y_P = \{y \in Y |\ y \text{ belongs to a finite orbit of } \psi\},$$

and

$$Y_{RI} = Y \setminus Y_P = \{y \in Y |\ y \text{ is of type (B) or (C)}\}.$$

Higman proved the following Theorem. .

Theorem 3.1.1. *[Hig74, Theorem 9.5 and its proof] Let ψ be an element of $G_{2,1}$. Then with the notation above, the following hold.*

1. *$V_{2,1}$ is a free product of the subalgebras V_P and V_{RI}.*
2. *The subalgebras V_P and V_{RI} are ψ-invariant.*
3. $$V_P = Y_P\langle A\rangle\langle\lambda\rangle$$
   and
   $$V_{RI} = Y_{RI}\langle A\rangle\langle\lambda\rangle$$
4. *Let θ and φ be elements of $G_{2,1}$. Then $\theta^{-1}\psi\theta = \varphi$ if and only if*
   - *$\theta_P = \theta|_{V_{P,\psi}}$ is a map from $V_{P,\psi}$ to $V_{P,\varphi}$ and $\theta_{RI} = \theta|_{V_{RI,\psi}}$ is a map from $V_{RI,\psi}$ to $V_{RI,\varphi}$, such that*
   - *$\theta = \theta_P * \theta_{RI}$, as a map from $V_{2,1} = V_{P,\psi} * V_{RI,\psi}$ to $V_{P,\varphi} * V_{RI,\varphi} = V_{2,1}$ and*
   - *writing $\psi_P = \psi_{V_{P,\psi}}$, $\varphi_P = \varphi_{V_{P,\varphi}}$, $\psi_{RI} = \psi_{V_{RI,\psi}}$ and $\varphi_{RI} = \varphi_{V_{RI,\varphi}}$, we have*
   $$\theta_P^{-1}\,\psi_P\,\theta_P = \varphi_P \text{ and } \theta_{RI}^{-1}\,\psi_{RI}\,\theta_{RI} = \varphi_{RI}.$$

Example 3.1.2. Let ψ be as in Example 2.5.8. Then ψ_P is an automorphism of $\{x\alpha_2\alpha_1, x\alpha_2^2\}\langle A\rangle\langle\lambda\rangle$ defined by,

$$x\alpha_2\alpha_1 \mapsto x\alpha_2^2, x\alpha_2^2 \mapsto x\alpha_2\alpha_1$$

and ψ_{RI} an isomorphism of $\{x\alpha_1^3, x\alpha_1\alpha_2, x\alpha_1^2\alpha_2\}\langle A\rangle\langle\lambda\rangle$ to $\{x\alpha_1^2, x\alpha_1\alpha_2^2, x\alpha_1\alpha_2\alpha_1\}\langle A\rangle\langle\lambda\rangle$ defined by,

$$x\alpha_1^3 \mapsto x\alpha_1^2, x\alpha_1\alpha_2 \mapsto x\alpha_1\alpha_2^2, x\alpha_1^2\alpha_2 \mapsto x\alpha_1\alpha_2\alpha_1.$$

Part 4 of Theorem 3.1.1 allows us to consider two parts of an element of $G_{2,1}$ separately. In fact V_P and V_{RI} are both isomorphic to $V_{2,1}$, so we may regard θ_P and θ_{RI} as automorphisms of $V_{2,1}$ via this identification.

Let ψ and ϕ be elements of $G_{2,1}$, write $V_1 = V_{RI,\psi}$ and $V_2 = V_{RI,\phi}$, and write $\psi_1 = \psi_{RI}$ and $\phi_1 = \phi_{RI}$. (Alternatively, let $V_1 = V_{P,\psi}$ and $V_2 = V_{P,\phi}$, and let $\psi_1 = \psi_P$ and $\phi_1 = \phi_P$; it doesn't affect what follows.)

Then $\psi_1 \in \mathrm{Aut}(V_1)$ and $\phi_1 \in \mathrm{Aut}(V_2)$ and V_i is isomorphic to $V_{2,1}$, for $i = 1, 2$. Let $f : V_1 \to V_{2,1}$ and $g : V_2 \to V_{2,1}$ be fixed isomorphisms, and define $\hat{\psi} = f^{-1}\psi f$ and $\hat{\phi} = g^{-1}\phi g$. Then $\hat{\psi}$ and $\hat{\phi}$ are elements of $G_{2,1}$ and the diagrams in Figure 3.1.0.1 commute.

Now $\hat{\psi} \sim \hat{\phi}$ if and only if there exists $\rho \in G_{2,1}$ such that $\rho^{-1}\hat{\psi}\rho = \hat{\phi}$

$$\begin{array}{ccc} V_{2,1} & \xrightarrow{\hat{\psi}} & V_{2,1} \\ \uparrow f & & \uparrow f \\ V_1 & \xrightarrow{\psi_1} & V_1 \end{array} \qquad \begin{array}{ccc} V_{2,1} & \xrightarrow{\hat{\phi}} & V_{2,1} \\ \uparrow g & & \uparrow g \\ V_2 & \xrightarrow{\phi_1} & V_2 \end{array}$$

Figure 3.1.0.1: Commutative diagrams

if and only if $\rho^{-1}f^{-1}\psi_1 f\rho = g^{-1}\phi_1 g$

if and only if $g\rho^{-1}f^{-1}\psi_1 f\rho g^{-1} = \phi_1$

if and only if $\theta^{-1}\psi_1\theta = \phi_1$, where $\theta = f\rho g^{-1}$.

Here θ is an isomorphism of V_1 to V_2, so could be taken to be either θ_P or θ_{RI} in Theorem 3.1.1, as appropriate. Of course, given such a θ, we have $\rho = f^{-1}\theta g$, satisfying all the above.

Note that, if $u, v \in V_{2,1}$ then there exist $a, b \in V_1$ such that $u = af$ and $v = bf$. In this case $u\psi^n = v$ if and only if $u\psi^n f = vf$ if and only if $uf\hat{\psi}^n = vf$. It follows that, if $V_1 = V_P$ then $\hat{\psi}$ is periodic, while if $V_1 = V_{RI}$ then $\hat{\psi}$ is regular infinite.

Combining this with Theorem 3.1.1 gives the required decomposition of the conjugacy problem into the conjugacy problem for periodic and for regular infinite elements, separately. At least in principle: the question of finding f and g algorithmically still remains. It's true that any isomorphism could be chosen in each case, but then the maps $\hat{\psi}$ and $\hat{\phi}$ have to be given with respect to suitable bases, and this will be unpleasant unless f and g are chosen sensibly.

First we give an outline of the strategy we shall adopt; and then we shall verify that all the steps do in fact work. The process described here is only for the regular infinite part of an automorphism; as everything works in the same way for the periodic part.

Given ψ in semi-normal form with respect to X, and $Y = X\psi$, let X_{RI} and Y_{RI} be the regular infinite parts of these bases and let $V_0 = V_{RI}$. Find a basis $B_0 \subseteq \mathbf{x}\langle A\rangle$ for V_0, such that if v is any element of X_{RI} or Y_{RI} then $v = b\Gamma$, for some $b \in B_0$ and $\Gamma \in \langle A\rangle$. Next contract the basis B_0 as much as possible: that is until it contains no pair of elements $x\Gamma\alpha_1$ and $x\Gamma\alpha_2$, $x \in \mathbf{x}$. Denote by Z_0 the resulting basis of V_0. Next choose a maximal length element of Z_0, say $z = x\Gamma\alpha_i$, where $x \in \mathbf{x}$, $\Gamma \in \langle A\rangle$, and replace it by $x\Gamma$. Let V_1 be the algebra generated by $Z_0\backslash\{z\} \cup \{x\Gamma\}$ and define a new map ψ_1, from V_1 to itself, obtained from the map X_{RI} to Y_{RI} as follows. Given v in X_{RI} or Y_{RI}, if v has the form $x\Gamma\alpha_i\Delta$, $\Gamma, \Delta \in \langle A\rangle$ then replace it with $x\Gamma\Delta$. Having done this for all such v, map the new sets X_{RI} and Y_{RI} to each other in the same

order as before. Now repeat the process starting with ψ_1 instead of ψ_{RI}. Continue for as long as possible. We shall verify below that this process does indeed result in an isomorphism from V_{RI} to $V_{2,1}$ such that the automorphism $\hat{\psi}$ corresponding to ψ, as above, is automatically given as a map between two bases of $V_{2,1}$ (contained in $\mathbf{x}\langle A\rangle$).

Example 3.1.3. Let ψ be an element of $G_{2,1}$ in quasi-normal form with respect to the basis,

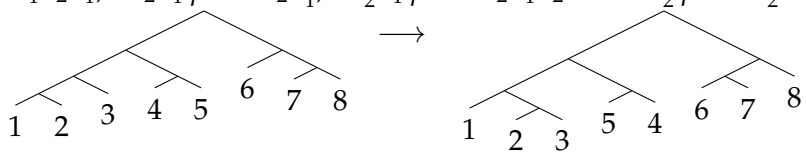
$$Y = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1, x\alpha_2^3\}$$

and defined by the bijection with the basis

$$Z = \{x\alpha_1^3, x\alpha_1^2\alpha_2\alpha_1, x\alpha_1^2\alpha_2^2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$$

given by $x\alpha_1^4\psi = x\alpha_1^3$, $x\alpha_1^3\alpha_2\psi = x\alpha_1^2\alpha_2\alpha_1$, $x\alpha_1^2\alpha_2\psi = x\alpha_1^2\alpha_2^2$, $x\alpha_1\alpha_2\alpha_1\psi = x\alpha_1\alpha_2^2$, $x\alpha_1\alpha_2^2\psi = x\alpha_1\alpha_2\alpha_1$, $x\alpha_2\alpha_1\psi = x\alpha_2\alpha_1^2$, $x\alpha_2^2\alpha_1\psi = x\alpha_2\alpha_1\alpha_2$ and $x\alpha_2^3\psi = x\alpha_2^2$.

ψ :



The subsets of elements of Y and Z in infinite orbits are

$$Y_{RI} = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1, x\alpha_2^3\},$$

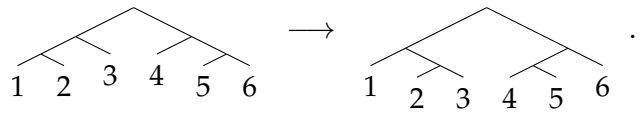
and

$$Z_{RI} = \{x\alpha_1^3, x\alpha_1^2\alpha_2\alpha_1, x\alpha_1^2\alpha_2^2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}.$$

The subset of elements of Y and Z in finite orbits is

$$Y_P = \{x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2\} = Z_P.$$

We can see that ψ_{RI} is a map from $Y_{RI}\langle A\rangle\langle\lambda\rangle$ to $Z_{RI}\langle A\rangle\langle\lambda\rangle$. For ψ_{RI} we can contract the bases Y and Z so that we remove part of our diagram to form the regular infinite element $\widehat{\psi}$ given by the tree pair,



.

In a sense we are "pruning" our tree pair at the edge going from $x\alpha_1$ to $x\alpha_1^2$ and contracting the elements $x\alpha_1^2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2$ to the element $x\alpha_1$.

Before we describe the steps of this process in detail we establish some preliminary results.

Lemma 3.1.4. *Let V be a subalgebra of $V_{2,1}$ and let Y be a basis of V. Then there exists a basis Z of V such that*

1. *for all $y \in Y$ there is $z \in Z$ such that z is an initial segment of y and*
2. *if $z_1, z_2 \in Z$ then $z_1 z_2 \lambda \notin \mathbf{x}\langle A\rangle$.*

Such a basis Z is called a contracted *basis of V, with respect to Y.*

Proof. If Y is contracted (that is the second condition holds for Y) then we may take $Y = Z$. Otherwise there exist $y_1, y_2 \in Y$ and Γ in $\langle A\rangle$ such that $y_i = x\Gamma\alpha_i$, $i = 1, 2$, $x \in \mathbf{x}$. Then the contraction $Y \setminus \{y_1, y_2\} \cup \{x\Gamma\}$ is a basis for V and has fewer elements than Y. Continuing this way we eventually obtain a contracted basis Z. □

Lemma 3.1.5. *Let X and Y be free bases of a subalgebra V of $V_{2,1}$ (with $X, Y \subseteq \mathbf{x}\langle A\rangle$). Then there exists a basis B of V such that, $X \cup Y \subseteq B\langle A\rangle$ (and $B \subseteq \mathbf{x}\langle A\rangle$).*

Proof. From Lemma 2.4.21 there exist subsets X' and Y' of $\mathbf{x}\langle A\rangle$, such that $\hat{X} = X \cup X'$ and $\hat{Y} = Y \cup Y'$ are expansions of $\mathbf{x}$. Now, if $x \in X$, from Lemma 2.4.21 again, there exists $y \in \hat{Y}$ such that one of x and y is an initial segment of the other. If $y \in Y'$ and x is an initial segment of y then $y = x\Gamma$, for some $\Gamma \in \langle A\rangle$, so $y \in X\langle A\rangle \subseteq V$ and hence $y = y_1\Delta$, where $y_1 \in \hat{Y}$, $y_1 \neq y$, contradicting Lemma 2.4.21. If y is an initial segment of x then interchanging roles of X and X' and of Y and Y', we have again a contradiction. Hence, for all $x \in X$ there exists y in Y such that one of x and y is an initial segment of the other. The analogous statement holds for elements of Y.

Now let $Z = X \cap Y$, $X^{(S)} = \{x \in X | x \notin Y\langle A\rangle\}$ and $Y^{(S)} = \{y \in Y | y \notin X\langle A\rangle\}$. We shall show that

$$B = Z \cup X^{(S)} \cup Y^{(S)}$$

is a free basis for V. From the previous paragraph, every element $x \in X$ is in $Y\langle A\rangle$ or $X^{(S)}$. If $x \notin Z \cup X^{(S)}$ then $x \in Y\langle A\rangle$ so $x = y\Gamma$, for some $\Gamma \in \langle A\rangle$. If $y \notin Y^{(S)}$ then $y = x_1\Delta$, for some $x_1 \in X$ and $\Delta \in \langle A\rangle$, so $x = y\Gamma = x_1\Gamma\Delta$, and Lemma 2.4.21 implies that $x = x_1$ and Γ and Δ are trivial. However, this means that $x \in Z$, contrary to the choice of x. Thus, $x \notin Z$ and $x \notin X^{(S)}$ implies that $x \in Y^{(S)}\langle A\rangle$. Therefore B generates V. From the definition of B it follows that no element of B is an initial segment of another. Therefore B is a basis for V, as claimed. As B has all the properties listed in the Lemma, this completes the proof. □

Now, as above assume $\psi \in G_{2,1}$ is in semi-normal form with respect to X, let $Y = X\psi$, let $X_0 = X_{RI}$ and $Y_0 = Y_{RI}$ be the regular infinite parts of these bases and let $V_0 = V_{RI}$ and let $\psi_0 = \psi_{RI}$. As in the proof of Lemma 3.1.5, let $X_0^{(S)} = \{x \in X_0 | x \notin Y_0\langle A\rangle\}$ and $Y_0^{(S)} = \{y \in Y_0 | y \notin X_0\langle A\rangle\}$. Then, from Lemma 3.1.5, $B_0 = (X_0 \cap Y_0) \cup X_0^{(S)} \cup Y_0^{(S)}$ is a free basis for V_0, and every element of $X_0 \cup Y_0$

belongs to $B_0\langle A\rangle$. From Lemma 3.1.4 we may choose a contracted basis Z_0 for V_0 with respect to B_0.

Let z be an element of maximal length in Z_0. Then $z = x\Gamma\alpha_i$, for some $x \in \mathbf{x}$, $\Gamma \in \langle A\rangle$ and $i \in \{1,2\}$. By definition of contracted basis, $x\Gamma\alpha_j \notin Z_0$, for $j \neq i$. Also, $x\Gamma\alpha_j\Delta \notin Z_0$, for all non-trivial $\Delta \in \langle A\rangle$, as z is of maximal length. Therefore, for all $u \in Z_0 \setminus \{z\}$, no initial segment of u is equal to $x\Gamma$. (Here we use Lemma 2.4.21 again.)

Iteration process: Define $f_0 : V_0 \to V_{2,1}$ by defining it on Z_0 as the map given by $uf_0 = u$, if $u \neq z$ and $zf_0 = x\Gamma$. Let $B_1 = Z_0f_0 = Z_0 \setminus \{z\} \cup \{x\Gamma\}$ and let $V_1 = B_1\langle A\rangle\langle\lambda\rangle$. Observe that no element of B_1 is an initial segment of another: if u is not equal to z and is an initial segment of $x\Gamma$ then it's an initial segment of $x\Gamma\alpha_i = z$, a contradiction; while if $x\Gamma$ is an initial segment of u then, as $x\Gamma\alpha_j\Delta \notin Z_0$, for all $\Delta \in \langle A\rangle$, it follows that $z = x\Gamma\alpha_i$ is an initial segment of u, again a contradiction. This means that B_1 is a free basis for V_1. Thus f_0 is an isomorphism (as it maps a free basis of V_0 bijectively to a free basis of V_1).

Next, let $\psi_1 = f_0^{-1}\psi f_0$, so $\psi_1 \in \mathrm{Aut}(V_1)$, let $X_1 = X_0f_0$ and let $Y_1 = Y_0f_0$. For $v \in X_1$ we have (unique) $u \in X_0$ such that $uf_0 = v$. Then $v\psi_1 = (uf_0)f_0^{-1}\psi_0f_0 = u\psi f_0 = wf_0 = y$, for some $w \in Y_0$ and $y \in Y_1$ such that $wf_0 = y$.

If $V_1 \neq V_{2,1}$, take a contracted basis Z_1 for B_1. As $V_1 \neq V_{2,1}$ this basis Z_1 is not equal to $\mathbf{x}$, so the process we may repeated, starting with ψ_1 and Z_1 instead of ψ_0 and Z_0. As $\sum_{b\in B_1}|b| < \sum_{b\in B_0}|b|$ the process must come to a halt after say n repetitions, at which point we have a sequence $V_0, \ldots, V_n$ of subalgebras and a sequence $f_0, \ldots, f_{n-1}$ of isomorphisms such that f_i maps V_{i-1} to V_n and $V_n = V_{2,1}$. Moreover we have bases X_i and Y_i for V_i, such that $\psi_i = f_{i-1}^{-1}\psi_{i-1}f_{i-1}$ maps X_i bijectively to Y_i. Setting $f = f_0 \cdots f_{n-1}$ we obtain $\psi_n = f^{-1}\psi_0 f$, $\psi_n \in G_{2,1}$, ψ_n maps X_n bijectively to Y_n and ψ_n is regular infinite. This ends the iteration process.

Algorithm 3.1.6. Let ψ be an element of $G_{2,1}$ in quasi-normal form with respect to the basis X with $X\psi = Y$.

Step 1: Find the sets $X_{RI} = V_{RI} \cap X$ and $X_P = V_P \cap X$, then $Y_{RI} = X_{RI}\psi$ and $Y_P = X_P\psi$.

Step 2: Either set $\psi_0 = \psi_{RI}$, $X_0 = X_{RI}$, $Y_0 = Y_{RI}$ and $V_0 = V_{RI}$ or $\psi_0 = \psi_P$, $X_0 = X_P$, $Y_0 = Y_P$ and $V_0 = V_P$. Find a basis B_0 for V_0 such that $X_0 \cup Y_0 \subseteq B_0\langle A\rangle$ (as in the proof of Lemma 3.1.5). Set $n = 0$ and $f = 1$.

Step 3: Find a contracted basis Z_n for B_n.

Step 4: Collapse Z_n as above (see **Iteration process**) to give a new basis B_{n+1} and a map f_n.

Step 5: Set $f = f_n f$.

Step 6: If B_{n+1} generates $V_{2,1}$ output f. Otherwise add 1 to n and repeat from step 3.

Remark 3.1.7. If ψ is in quasi-normal form with respect to X then it can be shown that the automorphism ψ_n is in quasi-normal form with respect to X_n.

Now that we have set up this terminology, we will use it in Algorithm 3.3.25.

Definition 3.1.8. Let ψ be an element of $G_{2,1}$. We shall say that ψ is *periodic* if and only if $V_{RI} = \emptyset$. We say that ψ is *regular infinite* if $V_P = \emptyset$.

Lemma 3.1.9. *Let ψ be an element of $G_{2,1}$, then ψ is a periodic element if and only if there exists a basis Y giving ψ in semi-normal form such that $Y\psi = Y$* i.e. *ψ permutes the elements of Y.*

Proof. If Y is a basis giving ψ in semi-normal form such that $Y\psi = Y$, then all elements of the basis are in a finite orbit. Therefore all elements of $V_{2,1}$ are in finite orbits, thus $V_{RI,\psi} = \emptyset$.

If $V_{RI,\psi} = \emptyset$, then there exists no characteristic elements in $V_{2,1}$. Since ψ is an element of $G_{2,1}$, then exists a basis Y giving ψ in semi-normal form. Since all orbits in $V_{2,1}$ are finite, no element y of Y is of type (B) or (C). Thus, by Lemma 2.5.13, $y \in Y$ belongs to a finite orbit which consists of elements of Y. □

Lemma 3.1.10. *Let ψ be a non-trivial element of $G_{2,1}$ in semi-normal form with respect to the basis Y, then the following are equivalent:*

- *ψ is regular infinite;*
- *no element of Y is in a finite orbit.*

Proof. If ψ is regular infinite then $V_{P,\psi} = \emptyset$ and no elements if $V_{2,1}$ are in a finite orbit. Since $Y \subset V_{2,1}$ then no element of Y is in a finite orbit.

If there exists no element of Y in a finite orbit, then $Y_1 =$ so $V_P =$, from Theorem 3.1.1. □

3.2 Conjugacy problems

In order to describe the conjugacy problem for a group we start with the definition of a group by a presentation, that is from a set of generators and defining relators.

Given a set S of symbols and a set R (possibly empty) of words in the symbols and their inverses (elements of the free monoid $(S \cup S^{-1})^*$), then G has presentation

$$\langle S|R\rangle,$$

if G is isomorphic to the quotient of a free group on S by the normal subgroup generated by the relations R.

However, as soon as we wish to determine more information about the group G defined by the presentation $\langle S|R\rangle$ we run into difficulties even if S and R are finite. One such problem is that the definition of equivalence of words used to obtain G is non-constructive. Therefore, the problem of deciding whether a word in $(S \cup S^{-1})^*$ defines the identity element becomes a non-trivial question. This problem is the first of the three fundamental decision problems formulated by Max Dehn [Dehn1911].

Dehn posed the following problems for a group G given by a presentation $\langle S|R\rangle$.

Word Problem: For an arbitrary word W in the generators S, decide in a finite number of steps whether W defines the identity element of G, or not.

Conjugacy Problem: For two arbitrary words W_1, W_2 in the generators S, decide in a finite number of steps, whether W_1 and W_2 define conjugate elements of G, or not.

Isomorphism Problem: For an arbitrary group G' defined by means of another presentation, decide in a finite number of steps whether G is isomorphic to G', or not.

The explicit solution (whenever it is possible) of the above problems is always dependent on a specific presentation (although the *existence* of a solution does not depend on a presentation, when we talk about finite presentations). Therefore, we always talk about the above problems, for a group G, assuming that it is given by a particular presentation.

In the case considered in this thesis we do something slightly different. Each element ψ of $G_{2,1}$ is uniquely represented by a pair of lists of elements Y and Z (up to reordering), where Y and Z are finite bases of the same cardinality; ψ is in quasi-normal form with respect to Y and the i^{th} element of Y maps to the i^{th} element of Z. To decide if two automorphisms are equal we check if these quasi-normal forms are the same.

Remark 3.2.1. Graham Higman [Hig74, Chapter 8] constructs an explicit finite presentation for the group $G_{2,1}$.

For the Higman-Thompson group $G_{2,1}$ the word and conjugacy problems were solved by Graham Higman in [Hig74, Section 9]. However, to extract the procedure for solving the conjugacy problem for the group $G_{2,1}$ from [Hig74, Section 9] is not straight forward and an explicit algorithm is not written down.

We, therefore, provide a description of the solution of the conjugacy problem for the group $G_{2,1}$. Next we consider the power conjugacy problem.

3.3 The conjugacy problem for $G_{2,1}$

By Theorem 3.1.1, ψ is conjugate to φ if and only if ψ_P is conjugate to φ_P and ψ_{RI} is conjugate to φ_{RI}.

We start by forming a series of lemmas, which will be referred to in the algorithm of Section 3.3.2.

3.3.1 Conjugacy for periodic and regular infinite elements

Periodic Elements

Definition 3.3.1. Let ψ be a torsion element of $G_{2,1}$ in quasi-normal form with respect to the basis Y. The *cycle type* of ψ is the *set* of lengths (in increasing order) of ψ-orbits of elements of Y *i.e.* for y in Y if m_1 is the smallest integer such that $y\psi^{m_1} = y$ then the length of the ψ-orbit of y is m_1. We write this set of lengths as an r-tuple $(m_1, m_2, ..., m_r)$.

Example 3.3.2. Let ψ be in quasi-normal form with respect to the basis Y

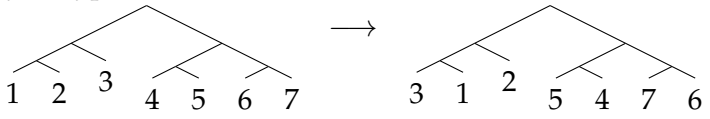
$$Y = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\alpha_1, x\alpha_2^3\},$$

and defined by the bijection,

$$x\alpha_1^3 \mapsto x\alpha_1^2\alpha_2,\ x\alpha_1^2\alpha_2 \mapsto x\alpha_1\alpha_2,\ x\alpha_1\alpha_2 \mapsto x\alpha_1^3,$$

$$x\alpha_2\alpha_1^2 \mapsto x\alpha_2\alpha_1\alpha_2,\ x\alpha_2\alpha_1\alpha_2 \mapsto x\alpha_2\alpha_1^2,\ x\alpha_2^2\alpha_1 \mapsto x\alpha_2^3,\ x\alpha_2^3 \mapsto x\alpha_2^2\alpha_1.$$

Then the cycle type of ψ is $(2, 3)$.

ψ : 

Our first step is to show that, if the periodic element ψ in quasi-normal form with respect to X has cycle type (n) (with multiplicity r on the basis X) and the periodic element φ in quasi-normal form with respect to Y has cycle type (n) (with no multiplicity on the basis Y) then ψ is conjugate to φ. The following lemma follows from the work of [Hig74, Section 6].

Lemma 3.3.3. *Let ψ, φ be periodic elements of $G_{2,1}$. Suppose that ψ is in quasi-normal form with respect to a basis X of size rn, φ is in quasi-normal form with respect to Y of size n and that each element ψ, φ has cycles type (n) with respect to these bases. Then there exists an element ρ of $G_{2,1}$ which maps X to an $n(r-1)$ fold expansion Y' of Y such that $\rho^{-1}\psi\rho = \varphi$.*

Proof. Without loss of generality, let ψ be in quasi-normal form with respect to the basis

$$X = \{x_0, ..., x_{n-1}, ..., x_{rn-n}, ..., x_{nr-1}\},$$

defined by $x_{in+j}\psi = x_{in+(j+1)_{\text{mod } n}}$ for $i = 0, ..., r-1$ and $j = 0, ..., n-1$, where $(j+1)_{\text{mod } n}$ means take $j+1$ mod n.

Let φ be in quasi-normal form with respect to the basis $Y = \{y_0, ..., y_{n-1}\}$ and defined by $y_k\varphi = y_{(k+1)_{\text{mod } n}}$ for $k = 0, ..., n-1$.

Let Y' be a basis of $V_{2,1}$ which is a $n(r-1)$-fold expansion of Y of the form $\{y_j\Gamma_i\}$ for $i = 0, ..., r-1$, $j = 0, ..., n-1$ and $\Gamma_i \in \langle A \rangle$ such that $y_j\Gamma_0$,....,$y_j\Gamma_{r-1}$ is an $(r-1)$-fold expansion of y_j. Define a map ρ by:

$$x_{in+j} \mapsto y_j\Gamma_i,$$

for $j = 0, ..., n-1$, $i = 0, ..., r-1$. Thus, ρ is a bijective map

$$\rho : X \to Y',$$

of bases, where $|X| = |Y'| = rn$ and thus ρ is an element of $G_{2,1}$.

We now check that the equation $\psi\rho = \rho\varphi$ holds.

1. We take the basis X and apply ψ then ρ. Thus, we have

$$x_{in+j}\psi\rho = x_{in+(j+1)_{\text{mod } n}}\rho = y_{(j+1)_{\text{mod } n}}\Gamma_i,$$

   for $j = 0, ..., n-1$ and $i = 0, ..., r-1$.

2. We take the basis X and apply ρ then φ. Thus, we have

$$x_{in+j}\rho\varphi = y_j\Gamma_i\varphi = y_j\varphi\Gamma_i = y_{(j+1)_{\text{mod } n}}\Gamma_i,$$

   for $j = 0, ..., n-1$ and $i = 0, ..., r-1$.

Hence, ρ conjugates ψ to φ. □

The second step is to show that, if the periodic element ψ in quasi-normal form with respect to X has cycle type $(n_1, ..., n_m)$ (with multiplicity's $r_1, ..., r_m$ on the basis X) and the periodic element φ in quasi-normal form with respect to Y has cycle type $(n_1, ..., n_m)$ (with no multiplicity's on the basis Y) then ψ is conjugate to φ.

Lemma 3.3.4. *Let ψ, φ be periodic elements of $G_{2,1}$. Suppose that ψ is in quasi-normal form with respect to a basis X of size $\sum_{i=1}^{m} r_i n_i$, φ is in quasi-normal form with respect to a basis Y of size $\sum_{i=1}^{m} n_i$, $r_i n_i$ elements of X have ψ-orbits of length n_i and n_i elements of Y*

have φ-orbits of length n_i. Then there exists a map ρ from X to some $(\sum_{i=1}^{m} n_i(r_i-1))$-fold expansion Y' of Y that is an element of $G_{2,1}$ such that $\rho^{-1}\psi\rho = \varphi$.

Proof. The proof follows the same method of the proof of Lemma 3.3.3, except we start (without loss of generality) with a basis for ψ of the form,

$$X = \{x_{n_1,0}, ..., x_{n_1,n_1-1}, ..., x_{n_1,r_1n_1-n_1}, ..., x_{n_1,n_1r_1-1}, ...,$$

$$x_{n_m,0}, ..., x_{n_m,n_m-1}, ..., x_{n_m,r_mn_m-n_m}, ..., x_{n_m,n_mr_m-1}\},$$

such that $x_{n_l,i_ln_l+j_l}\psi = x_{n_l,i_ln_l+(j_l+1)_{\text{mod } n_l}}$ for $i_l = 0, ..., r_l-1$ and $j_l = 0, ..., n_l-1$ where $(j_l+1)_{\text{mod } n_l}$ means take j_l+1 mod n_l, for $l = 1, ..., m$.

Similarly, we let φ be in quasi-normal form with respect to the basis

$$Y = \{y_{n_1,0}, ..., y_{n_1,n_1-1}, ..., y_{n_m,0}, ..., y_{n_m,n_m-1}\}$$

and defined by $y_{n_l,k_l}\varphi = y_{n_l,(k_l+1)_{\text{mod } n_l}}$ for $k_l = 0, ..., n_l-1$ and $l = 1, ..., m$.

Let Y' be a basis of $V_{2,1}$ which is a $(\sum_{i=1}^{m} n_i(r_i-1))$-fold expansion of Y of the form $\{y_{n_l,j_l}\Gamma_{n_l,i_l}\}$ for $i_l = 0, ..., r_l-1$, $j_l = 0, ..., n_l-1$ and $\Gamma_{n_l,i_l} \in \langle A \rangle$. Define a map ρ by:

$$x_{n_l,i_ln_l+j_l} \mapsto y_{n_l,j_l}\Gamma_{n_l,i_l},$$

for $i_l = 0, ..., r_l-1$, $j_l = 0, ..., n_l-1$ and $l = 1, ..., m$. Thus, ρ is a bijective map

$$\rho : X \to Y',$$

of bases, where $|X| = |Y'| = \sum_{i=1}^{m} r_in_i$ and thus ρ is an element of $G_{2,1}$.

We now check whether the equation $\psi\rho = \rho\varphi$ holds.

1. We take the basis X and apply ψ then ρ. Thus, we have

$$x_{n_l,i_ln_l+j_l}\psi\rho = x_{n_l,i_ln_l+(j_l+1)_{\text{mod } n_l}}\rho = y_{n_l,(j_l+1)_{\text{mod } n_l}}\Gamma_{n_l,i_l},$$

   for $i_l = 0, ..., r_l-1$, $j_l = 0, ..., n_l-1$ and $l = 1, ..., m$.

2. We take the basis X and apply ρ then φ. Thus, we have

$$x_{n_l,i_ln_l+j_l}\rho\varphi = y_{n_l,j_l}\Gamma_{n_l,i_l}\varphi = y_{n_l,j_l}\varphi\Gamma_{n_l,i_l} = y_{n_l,(j_l+1)_{\text{mod } n_l}}\Gamma_{n_l,i_l},$$

   for $i_l = 0, ..., r_l-1$, $j_l = 0, ..., n_l-1$ and $l = 1, ..., m$.

Hence, ρ conjugates ψ to φ. □

A d-fold expansion of $\{x\}$ has cardinality $d+1$.

Lemma 3.3.5. *For any set $\{n_1, ..., n_m\} \subset \mathbb{N}$, there exists an element φ of $G_{2,1}$ such that φ is in quasi-normal form with respect to a basis Y of size $\sum_{i=1}^{m} n_i$, where n_i elements of Y have orbits of length n_i.*

Proof. Let Y be a basis of $V_{2,1}$ defined in the following way:

Let $Y_0 = \{y_1, ..., y_m\}$ be any $m-1$-fold expansion of $\{x\}$ *i.e.* $y_i = x\Gamma_i$ for $\Gamma_i \in \langle A \rangle$ for $i = 1, ..., m$.

Let $Y = \{y_{1,1}, ..., y_{1,n_1}, ..., y_{m,1}, ..., y_{m,n_m}\}$ be any expansion of Y_0 such that $y_{i,j} = x\Gamma_i\Delta_j$ for $\Delta_j \in \langle A \rangle$, $j = 0, ..., n_i - 1$.

Define φ in the following way,

$$y_{i,j}\varphi = y_{i,j+1 \mod n_i}.$$

It is clear that $Y\varphi = Y$ is a bijective map between two (identical) bases of $V_{2,1}$ and thus φ is an element of $G_{2,1}$. In fact, since no element of $y \in Y$ is in an incomplete orbit, by definition φ is in semi-normal form with respect to the basis Y and φ is a periodic element.

If we assume that φ is not in quasi-normal form with respect to the basis Y, then there exists a contraction of the basis Y, $Y^* = Y \setminus \{w\alpha_1, w\alpha_2\} \cup \{w\}$ such that φ is in semi-normal form with respect to Y^*.

However, by definition of the element φ above, any contraction of $w\alpha_1, w\alpha_2 \in Y$ will result in an incomplete finite orbit. Thus φ is in quasi-normal form with respect to Y. □

We are now able to state the following result which completely characterises conjugacy for periodic elements of $G_{2,1}$.

Proposition 3.3.6. *Let ψ and φ be torsion elements of $G_{2,1}$ in quasi-normal form with respect to the bases X and Y respectively. Then, ψ is conjugate to φ if and only if ψ and φ have the same cycle type.*

Proof. If we assume that ψ and φ have the same cycle type, then we can apply Lemmas 3.3.4 and 3.3.5, and hence ψ and φ are conjugate.

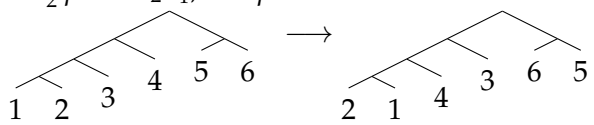
Assume ρ is any conjugator, conjugating ψ to φ. Then ρ maps the ψ-orbits in $V_{2,1}$ to φ-orbits in $V_{2,1}$. That is, if $u \in V_{2,1}$ and v is in the ψ-orbit of u then $v = u\psi^n$, for some $n \in \mathbb{Z}$. In this case $v\rho = u\psi^n\rho = u\rho\rho^{-1}\psi^n\rho = u\rho\varphi^n$. The converse also holds, by the same argument in reverse, so ρ maps ψ-orbits to ϕ-orbits, bijectively.

We will now look at the length of the φ-orbit $u\rho$. Suppose $u \in V_{2,1}$ and is in a ψ-orbit of length m. Then $u\rho\varphi^m = u\psi^m\rho = u\rho$ and thus $u\rho$ is in a φ orbit of length at most m. Given that ρ is an isomorphism, we can take $u\rho$ and see that $u\rho\rho^{-1} = u$ is in a ψ-orbit of length at least m. However, the ψ-orbit of u is of length m and by the above $u\rho$ must be in a φ-orbit of length m. □

Example 3.3.7. Let ψ be the periodic element of $G_{2,1}$ (in quasi-normal form with respect to the basis

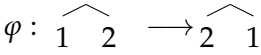
$$X = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}),$$

given by $x\alpha_1^4\psi = x\alpha_1^3\alpha_2$, $x\alpha_1^3\alpha_2\psi = x\alpha_1^4$, $x\alpha_1^2\alpha_2\psi = x\alpha_1\alpha_2$, $x\alpha_1\alpha_2\psi = x\alpha_1^2\alpha_2$, $x\alpha_2\alpha_1\psi = x\alpha_2^2$ and $x\alpha_2^2\psi = x\alpha_2\alpha_1$, *i.e.* ψ has order 2.

ψ : 

Let φ be a periodic element of $G_{2,1}$ (in quasi-normal form with respect to the basis

$$Y = \{x\alpha_1, x\alpha_2\}),$$

given by $x\alpha_1\varphi = x\alpha_2$ and $x\alpha_2\varphi = x\alpha_1$, *i.e.* φ has order 2. φ : 

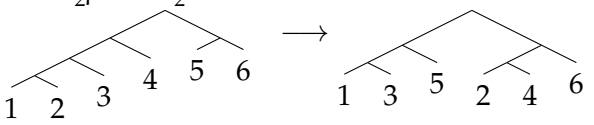
Then ψ is conjugate to φ. In fact we can construct a conjugator by applying the proof of Lemma 3.3.3. Let ρ be the element of $G_{2,1}$ defined by the bijection between bases

$$X = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\},$$

and

$$Y' = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$$

given by $x\alpha_1^4\rho = x\alpha_1^3$, $x\alpha_1^3\alpha_2\rho = x\alpha_2\alpha_1^2$, $x\alpha_1^2\alpha_2\rho = x\alpha_1^2\alpha_2$, $x\alpha_1\alpha_2\rho = x\alpha_2\alpha_1\alpha_2$, $x\alpha_2\alpha_1\rho = x\alpha_1\alpha_2$ and $x\alpha_2^2\rho = x\alpha_2^2$.

ρ : 

We can clearly see that ρ is of infinite order, since $x\alpha_1^3$ is a characteristic element with characteristic multiplier α_1 for ρ^{-1} (Theorem 2.5.18).

Regular Infinite Elements

In this section we consider regular infinite elements; if ψ is regular infinite then $V_{2,1} = V_{RI,\psi}$.

We begin with a necessary condition for two regular infinite elements to be conjugate.

Let ψ be a regular infinite element of $G_{2,1}$ in quasi-normal form with respect to X. By Lemma 2.5.9, ψ has finitely many semi-infinite orbits. For those semi-infinite orbits $\mathcal{O}$ that contain a characteristic element let $(m_{\mathcal{O}}, \Gamma_{\mathcal{O}})$ be the characteristic of $\mathcal{O}$ (see Definition 2.5.16). Recall that a semi-infinite orbit contains a characteristic

element if and only if it contains an element of type (B).

Since there are only finitely many semi-infinite orbits, the set

$$\{(m_{\mathcal{O}}, \Gamma_{\mathcal{O}}) | \text{ for } \mathcal{O} \text{ a semi-infinite orbit of } \psi \text{ containing an element of type (B)}\},$$

is finite. We now make a formal definition.

Definition 3.3.8. Let ψ be a regular infinite element of $G_{2,1}$ in quasi-normal form with respect to X.

Then

$$\mathcal{M}_\psi = \{(m, \Gamma) | \ (m, \Gamma) = (m_{\mathcal{O}}, \Gamma_{\mathcal{O}}), \text{ for } \mathcal{O} \text{ containing a characteristic element.}\},$$

is called the *set of characteristic multipliers and powers* for ψ.

Example 3.3.9. Let ψ be in quasi-normal form with respect to,

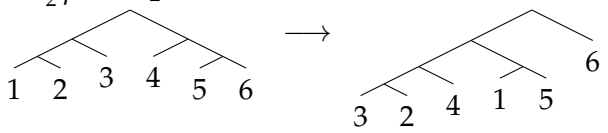
$$X = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1, x\alpha_2^3\}$$

defined by the bijection with the basis

$$Y = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2\},$$

given by $x\alpha_1^3\psi = x\alpha_1\alpha_2\alpha_1$, $x\alpha_1^2\alpha_2\psi = x\alpha_1^3\alpha_2$, $x\alpha_1\alpha_2\psi = x\alpha_1^4$, $x\alpha_2\alpha_1\psi = x\alpha_1^2\alpha_2$, $x\alpha_2^2\alpha_1\psi = x\alpha_1\alpha_2^2$ and $x\alpha_2^3\psi = x\alpha_2$.

ψ :



We have the following semi-infinite orbits,

$$\mathcal{O}_1 : x\alpha_1^3, x\alpha_1\alpha_2\alpha_1, x\alpha_1^5, ...$$

$$\mathcal{O}_2 : x\alpha_1\alpha_2, x\alpha_1^4, x\alpha_1\alpha_2\alpha_1^2, ...$$

$$\mathcal{O}_3 : ..., x\alpha_2^5, x\alpha_2^3, x\alpha_2$$

$$\mathcal{O}_4 : ..., x\alpha_2^6, x\alpha_2^4, x\alpha_2^2.$$

In this case we have $M_\psi = \{(2, \alpha_1^2), (-1, \alpha_2^2)\}$ since orbits $\mathcal{O}_1, \mathcal{O}_2$ and $\mathcal{O}_3$ contain elements of type (B). Orbit $\mathcal{O}_4$ contains a elements of type (C) but none of type (B). All other elements of in complete infinite orbits.

Lemma 3.3.10. *Suppose that ψ and φ are conjugate regular infinite elements of $G_{2,1}$ in quasi-normal form with respect to the bases X and Y respectively. Then the set of pairs $\mathcal{M}_\psi$ and*

$\mathcal{M}_\varphi$ coincide. Moreover, if $\rho \in G_{2,1}$ is such that $\rho^{-1}\psi\rho = \varphi$ then ρ maps an orbit which is semi-infinite with respect to X and has characteristic (m, Γ) to an orbit which is semi-infinite with respect to Y of the same characteristic.

Proof. Let ψ and φ be in quasi-normal form with respect to the bases X and Y respectively and let ρ be such that $\rho^{-1}\psi\rho = \varphi$. Then $\psi\rho = \rho\phi$. Thus, if u is an element of $X\langle A\rangle$ such that $u\psi^m = u\Gamma$, for some m and Γ, then

$$u\rho\varphi^m = u\psi^m\rho = u\Gamma\rho = u\rho\Gamma.$$

The same argument can be applied starting with an element $v \in Y\langle A\rangle$ and interchanging ψ and φ. Hence if u belongs to an orbit of ψ of characteristic (m, Γ) then $u\rho$ belongs to an orbit of φ of characteristic (m, Γ). Thus, from Lemma 2.5.19 an orbit which has a proper characteristic with respect to ψ maps to an orbit which has the same proper characteristic with respect to φ. □

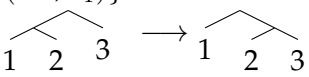
Example 3.3.11. Let ψ be in quasi-normal form with respect to,

$$X = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\}$$

defined by the bijection with the basis

$$Y = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\},$$

given by $x\alpha_1^2\psi = x\alpha_1$, $x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1$ and $x\alpha_2\psi = x\alpha_2^2$. In this case, the set $M_\psi = \{(1, \alpha_2), (-1, \alpha_1)\}$.

ψ : 

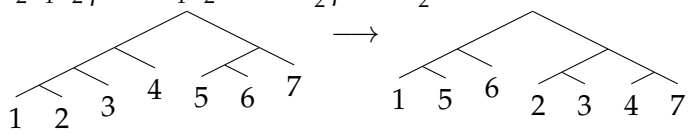
Define $\varphi = \rho^{-1}\psi\rho$ where ρ is as in Example 3.3.7. Then φ is in quasi-normal form with respect to,

$$Z = \{x\alpha_1^4, x\alpha_1^3\alpha_2, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$$

and defined by the bijection with the basis,

$$W = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\alpha_1, x\alpha_2^3\}$$

given by $x\alpha_1^4\varphi = x\alpha_1^3$, $x\alpha_1^3\alpha_2\varphi = x\alpha_2\alpha_1^2$, $x\alpha_1^2\alpha_2\varphi = x\alpha_2\alpha_1\alpha_2$, $x\alpha_1\alpha_2\varphi = x\alpha_2^2\alpha_1$, $x\alpha_2\alpha_1^2\varphi = x\alpha_1^2\alpha_2$, $x\alpha_2\alpha_1\alpha_2\varphi = x\alpha_1\alpha_2$ and $x\alpha_2^2\varphi = x\alpha_2^3$.

φ : 

The set $M_\varphi = \{(1, \alpha_2), (-1, \alpha_1)\}$ so coincides with M_ψ.

We now build up to Lemmas 3.3.15 and 3.3.16 which will be useful for the remainder of the subsection. However before this we will define an equivalence relation on the elements in a basis which gives an element of $G_{2,1}$ in quasi-normal form given by Graham Higman [Hig74, Page 75].

Definition 3.3.12. Let ψ be in semi-normal form with respect to X. The equivalence relation $\equiv$ on the elements of X, is defined to be the least equivalence relation such that $x \equiv x'$ whenever $x\Gamma$ and $x'\Delta$ are in the same ψ-orbit, for some $\Gamma, \Delta \in \langle A \rangle$.

Example 3.3.13. Let ψ be as in Example 3.3.11. Then, since $x\alpha_1^2\alpha_2\psi = x\alpha_1\alpha_2$ and $x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1$ we only have one equivalence class on X.

We shall now make some remarks about this definition. Let ψ be a regular infinite element in quasi-normal form with respect to X. Firstly, the initial relation $x \equiv_0 y$ if and only if $x\Gamma$ and $y\Delta$ belong to the same ψ-orbit (for some $\Gamma, \Delta \in \langle A \rangle$) is symmetric and reflexive but *not* transitive. Hence, the equivalence relation $\equiv$ (as defined above) on a subset S of $V_{2,1}$ relates x to y if and only if there exists an integer $n \geq 0$ and a sequence of elements $w_0 = x, ..., w_n = y$ in S, $\Gamma_0, ..., \Gamma_{n-1}, \Delta_1, ..., \Delta_n \in \langle A \rangle$ such that $w_i\Gamma_i$ and $w_{i+1}\Delta_{i+1}$ belong to the same orbit of ψ, for $i = 0, ..., n-1$.

Now that we have the definition of the relation $\equiv$, we will use this to make a finer decomposition of $V_{2,1}$.

Proposition 3.3.14. *Let ψ be a regular infinite element in quasi-normal form with respect to X. Let $X = \coprod_{i=1}^{n} \mathcal{X}_i$ where the $\mathcal{X}_i$ are the equivalence classes of $\equiv$ defined on X under the action of ψ.*

Then $V_{2,1}$ is the free product of the ψ-invariant subalegbras $V_1, ..., V_n$ where each V_i is the subalgebra generated by $\mathcal{X}_i$.

Proof. As ψ is regular infinite, the sets $\mathcal{X}_i$ partition X, so $V_{2,1}$ is the free product of the V_i's.

To show that V_i is ψ-invariant it suffices to show that if $x \in \mathcal{X}_i$ then $x\psi$ and $x\psi^{-1}$ are in V_i. To this end, choose $d \geq 0$ such that $x\psi\Gamma$ and $x\psi^{-1}\Gamma$ belong to $X\langle A \rangle$, for all $\Gamma \in \langle A \rangle$ of length d. Then, for Γ of length d, we have $x\psi\Gamma = y\Delta$ and $x\psi^{-1}\Gamma = z\Lambda$, for some $y, z \in X$ and $\Delta, \Lambda \in \langle A \rangle$. By definition then $y \equiv x \equiv z$, so $x, y, z \in \mathcal{X}_i$. This implies that $x\psi\Gamma = y\Delta \in V_i$ and $x\psi^{-1}\Gamma = z\Lambda \in V_i$. This holds for all Γ of length d, so from Lemma 2.5.5, $x\psi$ and $x\psi^{-1}$ belong to V_i, as required. Hence V_i is ψ invariant. □

Lemma 3.3.15. *Suppose ψ is a regular infinite element of $G_{2,1}$ in quasi-normal form with respect to X, and let $X\psi = Z$.*

If $X = \coprod_{i=1}^{n} \mathcal{X}_i$ and $Z = \coprod_{i=1}^{m} \mathcal{Z}_i$, where the $\mathcal{X}_i$ and $\mathcal{Z}_i$ are the equivalence classes of $\equiv$ defined on X and Z under the action of ψ and ψ^{-1} respectively, then $n = m$ and ψ maps the equivalence classes on X bijectively to the equivalence classes on Z. Moreover, if $\mathcal{X}_i\psi = \mathcal{Z}_j$ then $|\mathcal{X}_i| = |\mathcal{Z}_j|$.

Proof. Let $x_i, x_j \in X$. Since $X\psi = Z$, we have $x_i\psi = z_i$ and $x_j\psi = z_j$ for some $z_i, z_j \in Z$. First note that, if $k \in \mathbb{Z}$, and Γ, $\Delta \in \langle A \rangle$ such that $x_i\Gamma\psi^k = x_j\Delta$ then

$$z_i\Gamma\psi^k = x_i\psi\Gamma\psi^k = x_i\Gamma\psi^{k+1} = x_j\Delta\psi = x_j\psi\Delta = z_j\Delta,$$

so $z_i\Gamma = z_j\Delta\psi^{-k} = z_j\Delta(\psi^{-1})^k$.

Conversely, if $k \in \mathbb{Z}$, and Γ, $\Delta \in \langle A \rangle$ such that $z_i\Gamma = z_j\Delta\psi^{-k}$ then $z_i\Gamma\psi^k = z_j\Delta$ and

$$x_i\Gamma\psi^k = z_i\psi^{-1}\Gamma\psi^k = z_i\Gamma\psi^k\psi^{-1} = z_j\Delta\psi^{-1} = z_j\psi^{-1}\Delta = x_j\Delta.$$

Therefore, for all Γ, Δ in $\langle A \rangle$, $x_i\Gamma$ and $x_j\Delta$ belong to the same ψ-orbit if and only if $z_i\Gamma$ and $z_j\Delta$ belong to the same ψ^{-1}-orbit.

By definition of the equivalence relation $\equiv$ on X under the action of ψ, we have $x_i \equiv x_j$ if and only if there exists an integer $n \geq 0$, a sequence of elements $u_0 = x_i, \ldots, u_n = x_j$ of X, and elements $\Gamma_0, \ldots, \Gamma_{n-1}$, $\Delta_1, \ldots, \Delta_n$ in $\langle A \rangle$, such that $u_t\Gamma_t$ and $u_{t+1}\Delta_{t+1}$ belong to the same ψ-orbit, for $t = 0, \ldots, n-1$. Setting $v_t = u_t\psi$ we see from the first paragraph of the proof that this occurs if and only if the sequence $v_0 = z_i, \ldots, v_n = z_j$ has the property that $v_t\Gamma_t$ and $v_{t+1}\Delta_{t+1}$ belong to the same ψ^{-1}-orbit, for $t = 0, \ldots, n-1$. The latter holds if and only if $z_i \equiv z_j$ in the equivalence relation on Z given by ψ^{-1}. Hence ψ maps $\mathcal{X}_i$ bijectively to $\mathcal{Z}_i$, for $i = 1, \ldots, n$ (up to relabelling). As ψ maps X bijectively to Z it follows that the number of equivalence classes for X under ψ must equal the number of equivalence classes for Z under ψ^{-1}. □

Lemma 3.3.16. *Let ψ, $\mathcal{X}_i$ and $\mathcal{Z}_i$ be as in Lemma 3.3.15. Let $\theta_1, ..., \theta_n$ be maps defined by*

$$x\theta_i = \begin{cases} x\psi & \text{if } x \in \mathcal{X}_i, \\ x & \text{if } x \in \mathcal{X}_j \text{ for } i \neq j, \end{cases}$$

$i = 1, ..., n$.

Then each θ_i extends to an element of $G_{2,1}$ such that θ_i commutes with ψ and, for all $j = 1, ..., n$, θ_i, commutes with θ_j.

Proof. As θ_i is defined on a basis it extends to a unique endomorphism of $V_{2,1}$. Since $X = \coprod_{i=1}^{n} \mathcal{X}_i$ and $Z = \coprod_{i=1}^{n} \mathcal{Z}_i$, then (after reordering if necessary) $\mathcal{X}_i\psi = \mathcal{Z}_i$ for $i = 1, ..., n$ (from Lemma 3.3.15). Thus θ_i maps X to $(X \setminus \mathcal{X}_i) \cup \mathcal{Z}_i$. To show θ_i is an automorphism we need to show that $(X \setminus \mathcal{X}_i) \cup \mathcal{Z}_i$ is a basis and $|X| = |(X \setminus \mathcal{X}_i) \cup \mathcal{Z}_i|$.

By Lemma 3.3.15 $|X| = |(X \setminus \mathcal{X}_i) \cup \mathcal{Z}_i|$ and so it remains to prove that $(X \setminus \mathcal{X}_i) \cup \mathcal{Z}_i$ is a proper expansion of $\{x\}$.

From Lemma 3.3.15, $V_i = \mathcal{X}_i\langle A\rangle\langle\lambda\rangle$ is ψ invariant and $\mathcal{X}_i\psi = \mathcal{Z}_i$, for all i. From Lemma 2.4.21, V_i is freely generated by $\mathcal{X}_i$, and so also by $\mathcal{Z}_i$. Therefore V_i has bases $\mathcal{X}_i$ and $\mathcal{Z}_i$, for all i. As $V_{2,1} = V_1 * \cdots * V_n$ is free product, if Y_i is any basis for V_i then $\cup_{i=1}^{n} Y_i$ is a basis for $V_{2,1}$. In particular, if $J = \{1, \ldots, n\} \setminus \{i\}$ then $\mathcal{Z}_i \cup (\cup_{j\in J}\mathcal{X}_i) = (X \setminus \mathcal{X}_i) \cup \mathcal{Z}_i$ is a basis for $V_{2,1}$, as required. Therefore θ_i is an automorphism.

We now work for commutativity. Firstly, as $\mathcal{X}_i$ and $\mathcal{Z}_i$ are bases of V_i there exists a common expansion of $\mathcal{X}_i$ and $\mathcal{Z}_i$ for each $i = 1, ..., n$.

Finally, we can now show the commutativity of the elements θ_i and θ_j of $G_{2,1}$. Since $\mathcal{X}_i$ and $\mathcal{Z}_i$ generate V_i, for $i = j$ we have $\theta_i|_{V_i} = \psi|_{V_i}$, while for $j \neq i$ we have $\theta_i|_{V_j} = Id|_{V_i}$.

Now suppose $x_i \in \mathcal{X}_i$ and $x_i\psi = z_i \in \mathcal{Z}_i$. Then

$$x_i\psi\theta_i = z_i\theta_i = z_i\psi,$$

while

$$x_i\theta_i\psi = z_i\psi.$$

On the other hand, if $x_i \in \mathcal{X}_j$, $j \neq i$ then

$$x_j\psi\theta_i = z_j\theta_i = z_j$$

and

$$x_j\theta_i\psi = x_j\psi = z_j.$$

Hence $\psi\theta_i = \theta_i\psi$ for $i = 1, ..., n$ and similarly $\theta_i\theta_j = \theta_j\theta_i$ for $i \neq j$. □

Remark 3.3.17. We note that, if ψ and φ are conjugate by a conjugator ρ and θ commutes with ψ, then $\theta\rho$ is also a conjugator.

Lemma 3.3.18. *Let ψ and φ be regular infinite elements of $G_{2,1}$, in quasi-normal form with respect to the bases X and Y respectively.*

If ψ and φ are conjugate then, given $x_1, \ldots, x_n$ such that x_i is an element of type (B) in $\mathcal{X}_i$, there exists a conjugator ρ such that $x_i\rho$ is a terminal or initial element in a semi-infinite orbit for φ.

Proof. Since ψ and φ are conjugate, by Lemma 3.3.10 the set of characteristic multipliers for ψ and φ coincide and there exists an element ρ' such that $\rho'^{-1}\psi\rho' = \varphi$. Let x_i be the given element of type (B) in $\mathcal{X}_i$. Then, from Lemma 3.3.10, $x_i\rho'$ belongs to a semi-infinite φ-orbit, with the same characteristic as x_i. Let $y_i \in Z\langle A\rangle$ be an initial or

terminal element of this orbit. Then there exists j_i such that

$$x_i\rho' = y_i\varphi^{j_i}.$$

Thus, as ρ' is a conjugator, we can rewrite this as,

$$y_i = y_i\varphi^{j_i}\varphi^{-j_i} = x_i\rho'\varphi^{-j_i} = x_i\psi^{-j_i}\rho'.$$

For each equivalence class $\mathcal{X}_i$, we define each θ_i as in Lemma 3.3.16 and a new (potential) conjugator ρ by

$$\rho = (\prod_{i=1}^{n}\theta_i^{-j_i})\rho',$$

which is an element of $G_{2,1}$ and conjugates ψ to φ, since $\prod_{i=1}^{n}\theta_i^{-j_i}$ commutes with ψ.

We check, for each chosen $x_i \in \mathcal{X}_i$,

$$x_i\rho = x_i(\prod_{i=1}^{n}\theta_i^{-j_i})\rho' = x_i\theta_i^{-j_i}\rho' = x_i\psi^{-j_i}\rho' = y_i.$$

□

Definition 3.3.19. Let ψ and φ be regular infinite elements in quasi-normal form with respect to X and Y and $\mathcal{X}_i$ the equivalence classes on X.

We say $\mathcal{R}_i(\psi,\phi)$ is the set of pairs (x_i, y_i), where x_i is of type (B) in $\mathcal{X}_i$ and y_j is an initial or terminal element of a semi-infinite orbit of ϕ with the same characteristic as x_i.

The set $\mathcal{R}_i(\psi,\phi)$ is finite since the number of elements of type (B) in X and the number of semi-infinite orbits for φ is finite.

We define a new set $\mathcal{R}(\psi;\varphi)$ as follows. Given $(x_i, y_i) \in \mathcal{R}_i(\psi,\phi)$, $i = 1,\ldots,n$, let ρ_0 be the map from $\{x_1,\ldots,x_n\}$ to $\{y_1,\ldots,y_n\}$ given by

$$x_1\rho_0 = y_1, ..., x_{n-1}\rho_0 = y_{n-1} \text{ and } x_n\rho_0 = y_n.$$

(Note that from the definitions, the domain and range of ρ_0 are n-sets.) Then $\mathcal{R}(\psi;\varphi)$ is the set of all such maps.

Again, it is clear that this set of maps $\mathcal{R}(\psi;\varphi)$ is finite, since the number of type (B) elements of X and the number of semi-infinite orbits for φ is finite.

Lemma 3.3.20. *Given $\rho_0 \in R(\psi,\varphi)$, there are finitely many ways of extending ρ_0 to an element ρ of $G_{2,1}$ such that $\varphi = \rho^{-1}\psi\rho$. Moreover the existence of such an extension ρ can be effectively determined, and if such ρ exists then the images $y\rho$ can be effectively determined, for all $y \in X$.*

Proof. Throughout the proof, when we say ρ exists we mean that an extension ρ of ρ_0 to an element of $G_{2,1}$ exists and satisfies $\varphi = \rho^{-1}\psi\rho$. Note that we may effectively enumerate the initial part of the orbits of elements of φ and ψ, using the process of Lemma 2.5.25. Thus we may effectively construct the equivalence classes $\mathcal{X}_i$, and the sets $R_i(\psi, \varphi)$.

First consider a single equivalence class $\mathcal{X}_i$. We are given an element x_i of type (B) and an element y_i such that

$$x_i\rho_0 = y_i,$$

where y_i is an initial or terminal element of a semi-infinite orbit of φ with the same characteristic multiplier and power as x_i.

Let $x \in X$ of type (B). Then, by definition of $\equiv$, we have $x \in \mathcal{X}_i$ if and only if there exist elements $x_i = u_0, \ldots, u_n = x$ of X, elements $\Gamma_j, \Delta_j \in \langle A \rangle$ and $k_j \in \mathbb{Z}$ with $u_{j+1}\Delta_{j+1} = u_j\Gamma_j\psi^{k_j}$, for $j = 0, \ldots, n-1$. Before going any further we show that we may assume that u_j is of type (B), for all j. Suppose not, say u_j is of type (C). Then, by Lemma 2.5.13, there exist $k'_j \in \mathbb{Z}$, $\Gamma'_j \in \langle A \rangle$ and $u'_j \in X$ of type (B) such that $u_j\psi^{k'_j} = u'_j\Gamma'_j$. Now

$$u_{j-1}\Gamma_{j-1}\psi^{k_{j-1}+k'_j} = u_j\Delta_j\psi^{k'_j} = u'_j\Gamma'_j\Delta_j$$

and

$$u'_j\Gamma'_j\Gamma_j\psi^{k_j-k'_j} = u'_j\Gamma'_j\psi^{-k'_j}\Gamma_j\psi^{k_j} = u_j\Gamma_j\psi^{k_j} = u_{j+1}\Delta_{j+1},$$

so we may replace u_j by u'_j. Continuing this way, eventually all u_j will be of type (B).

We show, by induction on n, that there are finitely many possible values of $x\rho$, for an element $\rho \in G_{2,1}$ such that $x\varphi = x\rho^{-1}\psi\rho$ (where $x_i\rho = x_i\rho_0 = y_i$) and describe an effective procedure to enumerate the set of all such elements. Suppose first that $n = 1$, so $x = u_1$ and we have $\Gamma = \Gamma_0$, $\Delta = \Delta_1$ and $k = k_0$ such that $x_i\Gamma\psi^k = x\Delta$. Given that ρ exists, from Lemma 3.3.10, $x\rho$ belongs to a semi-infinite orbit $\mathcal{O}$ of φ with the same characteristic as x. Therefore (if ρ exists) there exists an element $(x, w) \in R_i(\psi, \varphi)$ such that w is the initial or terminal element of $\mathcal{O}$; and an integer l such that $w\varphi^l = x\rho$. This implies that

$$w\Delta\varphi^l = (x\Delta)\rho = x_i\Gamma\psi^k\rho = x_i\Gamma\rho\varphi^k = x_i\rho_0\varphi^k\Gamma,$$

so

$$w\Delta\varphi^{l-k} = x_i\rho_0\Gamma = y_i\Gamma. \tag{3.1}$$

Lemma 2.5.25 gives an effective procedure to determine whether an integer l satisfying (3.1) exists, and if so find it. Given ρ_0 and x, the integer k and the elements Γ and Δ are uniquely determined so, to decide whether an appropriate value $x\rho$ exists, we may check each pair (x, w) in the set $R_i(\psi, \varphi)$ to see if (3.1) holds for some l or not.

For each such w there is at most one l such that (3.1) has a solution and, as $R_i(\psi, \varphi)$ is finite, we may effectively enumerate the values $w\Delta\varphi^{l-k}$ that could be assigned to $x\rho$. Hence the result holds if $n = 1$.

Now assume that $n > 1$ and the result holds for all x related to x_i by a chain of length at most $n-1$. Then u_{n-1} is of type (B) and by assumption $u_{n-1}\rho$ may be given one of finitely many values, and we have a procedure to enumerate these values. Suppose then that $u_{n-1}\rho = v$. Now $x = u_n$ and we have $\Gamma_{n-1}, \Delta_n \in \langle A \rangle$ and $k_{n-1} \in \mathbb{Z}$ such that $u_{n-1}\Gamma_{n-1}\psi^{k_{n-1}} = x\Delta_n$. Applying the argument of the case $n = 1$ with u_{n-1}, Γ_{n-1}, Δ_n and v in place of x_i, Γ, Δ and y, we see that a finite set of possible values for $x\rho$ may be effectively determined. Therefore, by induction, the result holds for all $x \in \mathcal{X}_i$ of type (B).

Finally, if $x \in \mathcal{X}_i$ is of type (C), then by Lemma 2.5.13 there is a $z\Sigma$ in the orbit of x for some z of type (B) and $\Sigma \in \langle A \rangle$, *i.e.* $x\psi^p = z\Sigma$ for some integer p. Since we have already determined the possible images of all the type (B) elements in $\mathcal{X}_i$, if ρ exists we have, for each choice of $z\rho$,

$$x\rho = z\Sigma\psi^{-p}\rho = z\rho\Sigma\varphi^{-p}$$

and this determines the image of the type (C) element under ρ (uniquely once we have made our initial choice for the image of $z\rho$).

We carry out this process on each equivalence class in turn. An extension of ρ_0 exists only if the process results in a at least one possible value for each element of X. If the process returns a potential extension ρ of X then ρ is an extension of ρ_0, of the required type, if $X\rho$ is a basis of $V_{2,1}$ (i.e. an expansion of $\{x\}$); which may be verified effectively. □

We are now able to state the following result which completely characterizes conjugacy for regular infinite elements of $G_{2,1}$.

Proposition 3.3.21. *Let ψ and φ be regular infinite elements of $G_{2,1}$ in quasi-normal form with respect to X and Y respectively.*

Then, ψ is conjugate to φ if and only if there exists a map $\rho_0 \in \mathcal{R}(\psi; \varphi)$ such that ρ_0 extends to an element ρ of $G_{2,1}$ with $\rho^{-1}\psi\rho = \varphi$.

Proof. Obviously, if ρ_0 extends to an element of $G_{2,1}$ such that $\rho^{-1}\psi\rho = \varphi$, then ψ is conjugate to φ by ρ.

We now assume that ψ is conjugate to φ. Lemma 3.3.18 tells us that there exists a conjugator ρ such that for each equivalence class $\mathcal{X}_i$ there exists an element x_i of type (B) in $\mathcal{X}_i$ such that $x_i\rho$ is an initial or terminal element y_i of a semi-infinite orbit for φ.

We define ρ_0 to be the map $x_1 \mapsto y_1, ..., x_n \mapsto y_n$, where $y_i = x_i\rho$ for each $i = 1, ..., n$. Thus, ρ_0 is an element of the finite set $\mathcal{R}(\psi; \varphi)$. Now ρ_0 is the restriction of ρ to $\{x_1, \ldots, x_n\}$, so it certainly extends to ρ, as required. □

Example 3.3.22. Let ψ be in quasi-normal form with respect to the basis,

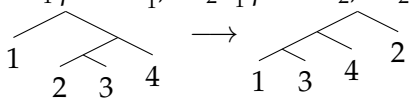
$$X = \{x\alpha_1, x\alpha_2\alpha_1^2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$$

and defined by the bijection with the basis

$$Z = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\}$$

given by $x\alpha_1\psi = x\alpha_1^3$, $x\alpha_2\alpha_1^2\psi = x\alpha_2$, $x\alpha_2\alpha_1\alpha_2\psi = x\alpha_1^2\alpha_2$, $x\alpha_2^2\psi = x\alpha_1\alpha_2$.

ψ :



This element has four semi-infinite orbits, two of which are right, each with associated characteristic multiplier and power pair $(1, \alpha_1^2)$,

$$\mathcal{O}_{1,\psi} = \{x\alpha_1\psi^k\}_{k\in\mathbb{N}_0}, \mathcal{O}_{2,\psi} = \{x\alpha_1^2\psi^k\}_{k\in\mathbb{N}_0},$$

and two of which are left each with associated characteristic multiplier and power pair $(-1, \alpha_1^2)$,

$$\mathcal{O}_{3,\psi} = \{x\alpha_2\alpha_1^2\psi^{-k}\}_{k\in\mathbb{N}_0}, \mathcal{O}_{4,\psi} = \{x\alpha_2\alpha_1^3\psi^{-k}\}_{k\in\mathbb{N}_0}.$$

The remaining elements in $X\langle A\rangle$ are in complete infinite orbits.

Let φ be in quasi-normal form with respect to the basis

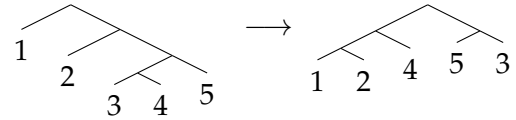
$$Y = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1^2, x\alpha_2^2\alpha_1\alpha_2, x\alpha_2^3\}$$

and defined by the bijection with the basis

$$W = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\}$$

given by $x\alpha_1\varphi = x\alpha_1^3$, $x\alpha_2\alpha_1\varphi = x\alpha_1^2\alpha_2$, $x\alpha_2^2\alpha_1^2\varphi = x\alpha_2^2$, $x\alpha_2^2\alpha_1\alpha_2\varphi = x\alpha_1\alpha_2$, $x\alpha_2^3\varphi = x\alpha_2\alpha_1$.

φ :



This element has four semi-infinite orbits, two of which are right, each with associated characteristic multiplier and power pair $(1, \alpha_1^2)$,

$$\mathcal{O}_{1,\varphi} = \{x\alpha_1\varphi^k\}_{k\in\mathbb{N}_0}, \mathcal{O}_{2,\varphi} = \{x\alpha_1^2\varphi^k\}_{k\in\mathbb{N}_0},$$

and two of which are left, each with associated characteristic multiplier and power pair $(-1, \alpha_1^2)$,

$$\mathcal{O}_{3,\varphi} = \{x\alpha_2^2\alpha_1^2\varphi^{-k}\}_{k\in\mathbb{N}_0}, \mathcal{O}_{4,\varphi} = \{x\alpha_2^2\alpha_1^3\varphi^{-k}\}_{k\in\mathbb{N}_0}.$$

The remaining elements in $Y\langle A\rangle$ are in complete infinite orbits.

Remark 3.3.23. The set $\mathcal{M}_\psi = \{(1, \alpha_1^2), (-1, \alpha_1^2)\}$ coincides with the set $\mathcal{M}_\varphi = \{(1, \alpha_1^2), (-1, \alpha_1^2)\}$.

There is only one equivalence class $\mathcal{X}_1 = X$ under the action of ψ as

$$x\alpha_2^2\psi = (x\alpha_1)\alpha_2,\ x\alpha_2\alpha_1\alpha_2\psi = (x\alpha_1)\alpha_1\alpha_2 \text{ and } (x\alpha_2\alpha_1^2)\alpha_2 = x\alpha_2^2\psi^{-1}.$$

Remark 3.3.24. The type (B) elements in X are $x\alpha_1$ and $x\alpha_2\alpha_1^2$.

The set $\mathcal{R}(\psi, \varphi)$ consists of the pairs $(x\alpha_1, x\alpha_1), (x\alpha_1, x\alpha_1^3), (x\alpha_2\alpha_1^2, x\alpha_2^2\alpha_1)$ and $(x\alpha_2\alpha_1^2, x\alpha_2^2\alpha_1^2)$.

Let us choose $x\alpha_1$ as our initial choice of the type (B) element. We therefore have two choices of initial element of a semi-infinite orbit of φ, which we we denote by

$$x\alpha_1\rho_1 = x\alpha_1 \text{ and } x\alpha_1\rho_2 = x\alpha_1^2,$$

where ρ_1 is one possible conjugator and ρ_2 is another.

We shall now apply Lemma 3.3.20 and Proposition 3.3.21 to determine if an actual conjugator exists. We determine the (potential) images of the other type (B) elements of X under the action of ρ_1 and ρ_2 first, then finish by determining the images of the type (C) elements of X.

The images of $x\alpha_2\alpha_1^2$: we first have that $(x\alpha_2\alpha_1^2)\alpha_2 = (x\alpha_1)\alpha_2\psi^{-2}$ and use equation 3.1 in the proof of Lemma 3.3.20 to determine the image of $x\alpha_2\alpha_1^2$ with $\Delta = \Gamma = \alpha_2$, $\rho_0 = \rho_1$ or ρ_2, $k = -2$ and either $w = x\alpha_2^2\alpha_1^2$ or $x\alpha_2^2\alpha_1^3$ so $w\alpha_2\varphi^{l+2} = x\alpha_1\rho_i\alpha_2$.

- (i) When $w = x\alpha_2^2\alpha_1^2$ we have,

$$x\alpha_2^2\alpha_1^2\alpha_2\varphi^{l_1+2} = x\alpha_1\rho_1\alpha_2$$
$$x\alpha_2\alpha_1\varphi^{l_1} = x\alpha_1\alpha_2$$

  which has no solutions (see Example 2.5.26).

(ii) When $w = x\alpha_2^2\alpha_1^3$ we have,

$$x\alpha_2^2\alpha_1^3\alpha_2\varphi^{l_2+2} = x\alpha_1\rho_1\alpha_2$$
$$x\alpha_1\alpha_2\varphi^{l_2} = x\alpha_1\alpha_2$$

and $l_2 = 0$. Therefore,

$$x\alpha_2^2\alpha_1^3\alpha_2 = x\alpha_1\alpha_2\psi^{-2}\rho_1 = x\alpha_2\alpha_1^2\alpha_2\rho_1,$$

and thus $x\alpha_2^2\alpha_1^3 = x\alpha_2\alpha_1^2\rho_1$.

- (i) When $w = x\alpha_2^2\alpha_1^2$ we have,

$$\begin{aligned} x\alpha_2^2\alpha_1^2\alpha_2\varphi^{l_1+2} &= x\alpha_1\rho_2\alpha_2 \\ x\alpha_2\alpha_1\varphi^{l_1} &= x\alpha_1^2\alpha_2 \\ x\alpha_2\alpha_1\varphi^{1} &= x\alpha_1^2\alpha_2 \end{aligned}$$

and $l_1 = 1$. Therefore,

$$\begin{aligned} x\alpha_2^2\alpha_1^3\alpha_2\varphi &= x\alpha_1\alpha_2\psi^{-2}\rho_2 \\ x\alpha_2^2\alpha_2 &= x\alpha_2\alpha_1^2\alpha_2\rho_2 \end{aligned}$$

and thus $x\alpha_2^2 = x\alpha_2\alpha_1^2\rho_2$.

(ii) When $w = x\alpha_2^2\alpha_1^3$ we have,

$$\begin{aligned} x\alpha_2^2\alpha_1^3\alpha_2\psi^{l_2+2} &= x\alpha_1\rho_2\alpha_2 \\ x\alpha_1\alpha_2\psi^{l_2} &= x\alpha_1^2\alpha_2 \end{aligned}$$

which has no solutions.

So $x\alpha_2^2\alpha_1^3 = x\alpha_2\alpha_1^2\rho_1$ and $x\alpha_2^2 = x\alpha_2\alpha_1^2\rho_2$ are the only possibilities. We now look at the elements of type (C) in X.

The images of $x\alpha_2^2$: we first have that $x\alpha_2^2\psi = (x\alpha_1)\alpha_2$ and assume $\psi\rho_i = \rho_i\varphi$ for $i = 1, 2$ to determine the image of $x\alpha_2^2$,

- $x\alpha_2^2\rho_1 = (x\alpha_1\rho_1)\alpha_2\varphi^{-1} = x\alpha_1\alpha_2\varphi^{-1} = x\alpha_2^2\alpha_1\alpha_2$;
- $x\alpha_2^2\rho_2 = (x\alpha_1\rho_2)\alpha_2\varphi^{-1} = x\alpha_1^2\alpha_2\varphi^{-1} = x\alpha_2\alpha_1$.

The images of $x\alpha_2\alpha_1\alpha_2$: we first have that $x\alpha_2\alpha_1\alpha_2\psi = (x\alpha_1)\alpha_1\alpha_2$ and assume $\psi\rho_i = \rho_i\varphi$ for $i = 1, 2$ to determine the image of $x\alpha_2\alpha_1\alpha_2$,

- $x\alpha_2\alpha_1\alpha_2\rho_1 = (x\alpha_1\rho_1)\alpha_1\alpha_2\varphi^{-1} = x\alpha_1\alpha_1\alpha_2\varphi^{-1} = x\alpha_2\alpha_1$;
- $x\alpha_2\alpha_1\alpha_2\rho_2 = (x\alpha_1\rho_2)\alpha_1\alpha_2\varphi^{-1} = x\alpha_1^2\alpha_1\alpha_2\varphi^{-1} = x\alpha_1\alpha_2$.

As the set $X\rho_1$ is not a basis, ρ_1 is not an automorphism. However, ρ_2 defined by the map,

$$x\alpha_1\rho_2 = x\alpha_1^2,\ x\alpha_2^2\rho_2 = x\alpha_2\alpha_1,\ x\alpha_2\alpha_1\alpha_2\rho_2 = x\alpha_1\alpha_2 \text{ and } x\alpha_2\alpha_1^2\rho_2 = x\alpha_2^2,$$

is an element of $G_{2,1}$ and must be a conjugator as can be checked.

3.3.2 Conjugacy Algorithm

All that is left is to combine Sections **Periodic Elements** and **Regular Infinite Elements** into one algorithm for any element of $G_{2,1}$.

Algorithm 3.3.25. Let ψ and φ be elements in quasi-normal form with respect to the basis bases X and Y.

Step 1: By Theorem 3.1.1, we split the elements ψ and φ into their periodic parts ψ_P, φ_P and their regular infinite parts ψ_{RI}, φ_{RI}.

Step 2: For ψ_{RI} and ψ_P use Algorithm 3.1.6 to construct isomorphisms f_{RI}, f_P and regular infinite element $\widehat{\psi_{RI}} = f_{RI}^{-1}\psi_{RI}f_{RI}$ and periodic element $\widehat{\psi_{RI}} = f_P^{-1}\psi_P f_P$. Similarly, use Algorithm 3.1.6 to construct isomorphisms g_{RI}, g_P and regular infinite element $\widehat{\varphi_{RI}} = g_{RI}^{-1}\varphi_{RI}g_{RI}$ and periodic element $\widehat{\varphi_{RI}} = g_P^{-1}\varphi_P g_P$.

Step 3: To the elements $\widehat{\psi_P}$, $\widehat{\varphi_P}$ of $G_{2,1}$, apply Proposition 3.3.6 to determine if there exists a conjugator ρ_P. If no conjugator exists, then ψ and φ are not conjugate;

Step 4: To the elements $\widehat{\psi_{RI}}$, $\widehat{\varphi_{RI}}$ of $G_{2,1}$ and apply Proposition 3.3.21 to determine if there exists a conjugator ρ_{RI}. If no conjugator exists, then ψ and φ are not conjugate;

Step 5: We combine Step's 3 and 4 and form a conjugator $\rho = \rho_P * \rho_{RI}$ by Theorem 3.1.1.

Theorem 3.3.26. *[Hig74, part of Theorem 9.3] The conjugacy problem is soluble in $G_{2,1}$.*

Proof. Apply Algorithm 3.3.25. □

3.4 Power conjugacy problem

The power conjugacy problem naturally arises when you have any group B and G is an HNN-extension given by

$$G = \langle a, B | \text{rel } B, a^{-1}Wa = V \rangle,$$

where W and V are words in the generators of B defining elements of the same order. It follows from [Mill71, Lemma 5] that if x and y are elements in B that are conjugate in G but not in B then x and y are conjugate in B to a power of W or V and hence in G to a power of W.

This motivates the study of the power conjugacy problem in groups.

Problem 3.4.1. [AS74] Given elements x, y of G, do there exist $a, b \in \mathbb{Z}$ and $z \in G$ such that $x^a = z^{-1}y^b z \neq 1$?

See [Lip66, AS74, Com77, Pride08] for references to this problem. The aim of this section is to answer this question for the Higman-Thompson group $G_{2,1}$ (Theorem 3.4.13).

Like the solution to the conjugacy problem, we will break the power conjugacy problem down into two cases; one for periodic elements and one for regular infinite elements. Then, we will construct an algorithm that will combine the two parts for a general pair of elements of $G_{2,1}$.

3.4.1 Power conjugacy for periodic and regular infinite elements

Torsion elements

Let ψ and φ be periodic elements of $G_{2,1}$ in quasi-normal form with respect to the bases X and Y, of order n and m respectively.

Then, to test whether ψ^a is conjugate to φ^b for $a, b \in \mathbb{Z}$, we can apply Proposition 3.3.6 to the pair ψ^a, φ^b for all $a \in \{1, ..., n\}$ and all $b \in \{1, ..., m\}$.

We define $\mathcal{PC}_P$ to be the set of all the pairs (a, b) that satisfy the condition that ψ^a is conjugate to φ^b.

Regular infinite elements

Let ψ and φ be regular infinite elements of $G_{2,1}$ in quasi-normal form with respect to the bases X and Y.

We want to compare the characteristic multipliers and powers of ψ with the characteristic multipliers and powers of ψ^a.

Lemma 3.4.2. *Let ψ be a regular infinite element of $G_{2,1}$ and a a non-negative integer. Then*

$$\mathcal{M}_{\psi^a} = \{(m/d, \Gamma^q) \mid (m, \Gamma) \in \mathcal{M}_\psi, \gcd(|m|, |a|) = d \text{ and } |a| = qd\}.$$

Proof. First we show that the right hand side is contained in the left hand side. If $(m, \Gamma) \in \mathcal{M}_\psi$ then there exists an element x of X (of type (B)) such that $x\psi^m = x\Gamma$. Suppose first that $a > 0$. If $d = \gcd(|m|, a)$, $p = m/d$, $q = a/d$ and $k = ma/d$, then $x(\psi^a)^p = x\psi^{mq} = x\Gamma^q$, (as mq has the same sign as m). If $a < 0$ then, from the above, with $d = \gcd(|m|, -a)$, $p = m/d$, $q = -a/d$ and $k = -ma/d$, we have $x\psi^{-ap} = x\Gamma^q$. In all cases therefore x is a characteristic element of ψ^a, with power m/d and multiplier Γ^q, where $d = \gcd(|m|, |a|)$ and $q = |a|/d$.

Conversely, if $x(\psi^a)^r = x\Delta$, with $\Delta \neq 1$ then, from Lemma 2.5.20, $m|ar$, which we can rewrite as $pd|qdr$, so $p|qr$. As $\gcd(|p|, q) = 1$, this implies $p|r$, so that $|m/d| =$

$|p| \leq |r|$. It follows that $(m/d, \Gamma^q)$ is in $\mathcal{M}_{\psi^a}$ and so we have

$$\mathcal{M}_{\psi^a} \supseteq \{(m, \Gamma^q) \mid (md, \Gamma) \in \mathcal{M}_\psi, d > 0, \gcd(|m|, q) = 1 \text{ and } |a| = qd\}.$$

On the other hand, suppose that $(r, \Delta) \in \mathcal{M}_{\psi^a}$ and assume ψ is in quasi-normal form with respect to X. (This does not necessarily mean ψ^a is in semi-normal form with respect to X.) Assume first that $a > 0$.Then, from Lemma 2.5.20, there exists $u \in V_{2,1}$ such that u is a characteristic element of ψ, with characteristic $(m, \Gamma) \in \mathcal{M}_\psi$ such that $m|ar$ and $\Delta = \Gamma^t$, where $ar = mt$, $t > 0$. Let $d = \gcd(|a|, |m|)$, $m = pd$ and $a = qd$. Then $dqr = pdt$, so $qr = pt$ and $\gcd(|p|, |q|) = 1$, so $r = pr'$ and $t = qt'$, for some r', t'. However, we have $u(\psi^a)^p = u\psi^{dpq} = u\psi^{mq} = u\Gamma^q$, and so, by definition of $(r, \Delta) \in \mathcal{M}_{\psi^a}$, we see that $|p| \geq |r|$, so $r' = \pm 1$. Since $a > 0$, $r' = 1$. It now follows that $r = p = m/d$ and $\Delta = \Gamma^q$, and (r, Δ) belongs to the set on the right hand side of the equality in the lemma. That is

$$\mathcal{M}_{\psi^a} \subseteq \{(m, \Gamma^q) \mid (md, \Gamma) \in \mathcal{M}_\psi, d > 0, \gcd(|m|, q) = 1 \text{ and } |a| = qd\}.$$

If $a < 0$ then the lemma follows by applying the result above to $\mathcal{M}_{\psi^{-1(-a)}}$, as for all $\theta \in G_{2,1}$ we have $(m, \Gamma) \in \mathcal{M}_\theta$ if and only if $(-m, \Gamma) \in \mathcal{M}_\theta^{-1}$. □

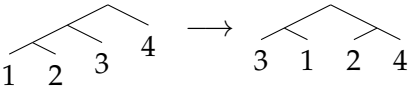
Example 3.4.3. Let ψ be a regular infinite element of $G_{2,1}$ in quasi-normal form with respect to

$$X = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2, x\alpha_2\},$$

and defined by a bijective map with

$$Y = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\},$$

given by the map $x\alpha_1^3\psi = x\alpha_1\alpha_2$, $x\alpha_1\alpha_2\psi = x\alpha_1^2$, $x\alpha_1^2\alpha_2\psi = x\alpha_2\alpha_1$ and $x\alpha_2\psi = x\alpha_2^2$.

ψ : 

Then $\mathcal{M}_\psi = \{(\text{-}2, \alpha_1), (1, \alpha_2)\}$.

We can look at ψ^2 in quasi-normal form with respect to

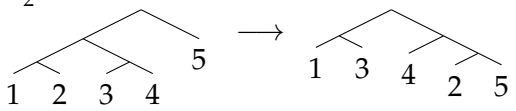
$$Z = \{x\alpha_1^3, x\alpha_1^2\alpha_2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2, x\alpha_2\}$$

and defined by a bijective map with

$$W = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\alpha_1, x\alpha_2^2\alpha_1, x\alpha_2^3\}$$

given by $x\alpha_1^3\psi^2 = x\alpha_1^2$, $x\alpha_1^2\alpha_2\psi^2 = x\alpha_2^2\alpha_1$, $x\alpha_1\alpha_2\alpha_1\psi^2 = x\alpha_1\alpha_2$, $x\alpha_1\alpha_2^2\psi^2 = x\alpha_2\alpha_1$ and $x\alpha_2\psi^2 = x\alpha_2^3$.

ψ^2 :



From Lemma 3.4.2, we have the following

$$\mathcal{M}_{\psi^a} = \{(m/d, \Gamma^q) \mid (m, \Gamma) \in \mathcal{M}_\psi, \gcd(|m|, |a|) = d \text{ and } |a| = qd\}.$$

Therefore, for:

- $(\text{-}2, \alpha_1) \in \mathcal{M}_\psi$ we have $m = \text{-}2$, $\Gamma = \alpha_1$, $\gcd(2,2) = 2 = d$ and thus $q = 1$. Hence, $(\text{-}2/2, \alpha_1^{2/2}) = (\text{-}1, \alpha_1) \in \mathcal{M}_{\psi^2}$.
- $(1, \alpha_2) \in \mathcal{M}_\psi$ we have $m = 1$, $\Gamma = \alpha_2$, $\gcd(1,2) = 1 = d$ and thus $q = 2$. Hence, $(1/1, \alpha_2^{2/1}) = (1, \alpha_2^2) \in \mathcal{M}_{\psi^2}$.

Thus, $\mathcal{M}_{\psi^2} = \{(1, \alpha_2^2), (\text{-}1, \alpha_1)\}$ (which can be checked above).

We now need Lemma 3.4.4 and Proposition 3.4.7 to allow us to find "minimal" pairs (a, b) such that ψ^a and φ^b are conjugate.

Lemma 3.4.4. *Let ψ and φ be regular infinite elements of $G_{2,1}$ and let c be an integer, such that c is coprime to m, for all $m \in \mathbb{Z}$ such that $(m, \Gamma) \in \mathcal{M}_\psi \cup \mathcal{M}_\varphi$. Then $\psi^c \sim \varphi^c$ if and only if $\psi \sim \varphi$.*

Proof. If $\psi \sim \varphi$ then it is immediate that $\psi^c \sim \varphi^c$. For the converse, observe that we may assume, without loss of generality, that $c > 0$. Suppose that ψ and φ are in quasi-normal form with respect to bases X and Y, respectively. From Lemma 3.4.2, $\mathcal{M}_{\psi^c} = \{(m, \Gamma^c) | (m, \Gamma) \in \mathcal{M}_\psi\}$ and $\mathcal{M}_{\varphi^c} = \{(m, \Delta^c) | (m, \Delta) \in \mathcal{M}_\varphi\}$.

Let u be an element of $X\langle A\rangle$ which is characteristic for ψ, with ψ-characteristic (m, Γ). Then, from Lemma 3.4.2 (and its proof), u has ψ^c-characteristic (m, Γ^c) and, as $\psi^c \sim \varphi^c$, its image $u\rho$ has φ^c-characteristic (m, Γ^c). Hence, from Lemma 3.4.2 again, $u\rho$ has φ-characteristic (m, Γ). As $\gcd(c, m) = 1$, there exist integers s and t such that $ms + ct = 1$. Since $\psi^c\rho = \rho\varphi^c$ we have, in the case where $s > 0$,

$$\begin{aligned} u\psi\rho &= u\psi^{ms+ct}\rho = (u(\psi^m)^s)\psi^{ct}\rho = u\Gamma^s\psi^{ct}\rho = u\Gamma^s\rho\varphi^{ct} \\ &= (u\rho)\Gamma^s\varphi^{ct} = (u\rho)\varphi^{ms}\varphi^{ct} = (u\rho)\varphi^{ms+ct} \\ &= u\rho\varphi. \end{aligned}$$

If $s < 0$ then we have $m(-s) + c(-t) = -1$, with $-s > 0$ and the argument above implies instead that $u\psi^{-1}\rho = u\rho\varphi^{-1}$. In this case, let $v = u\psi$, so v also has ψ-characteristic (m, Γ) and replacing u by v gives $v\psi^{-1}\rho = v\rho\varphi^{-1}$ from which it follows

that $u\psi\rho = u\rho\varphi$. This applies in particular to all elements of X of type (B). Let y' be an element of type (C); so there exists an element $y \in X$ of type (B) such that $y'\psi^k = y\Omega$, for some $k \in \mathbb{Z}$. Then $y' = y\Omega\psi^{-k}$, and $y\psi^j$ has the same ψ-characteristic as y, for all j: and so is a characteristic element for ψ. From the above then $y\psi^j\rho = (y\rho)\varphi^j$, for all j. Now

$$\begin{aligned} y'\psi\rho &= y\Omega\psi^{1-k}\rho = y\psi^{1-k}\rho\Omega = y\rho\varphi^{1-k}\Omega = y\rho\varphi^{-k}\varphi\Omega \\ &= y\psi^{-k}\rho\varphi\Omega = y\psi^{-k}\Omega\rho\varphi = y'\rho\varphi. \end{aligned}$$

Therefore, $y\psi\rho = y\rho\varphi$, for all $y \in X$, so $\psi \sim \varphi$. □

Definition 3.4.5. Let ψ be a regular infinite element of $G_{2,1}$ and let a be a positive integer. Define a map $\widehat{\psi}^a : \mathcal{M}_\psi \to \mathcal{M}_{\psi^a}$ by $\widehat{\psi}^a(m, \Gamma) = (p, \Gamma^\alpha)$, where $d = \gcd(|m|, a)$, $p = m/d$ and $\alpha = a/d$.

Example 3.4.6. Let ψ be as in Example 3.4.3 with $a = 2$. The map

$$\widehat{\psi}^2 : \mathcal{M}_\psi \to \mathcal{M}_{\psi^2}$$

can be calculated for each of the elements of $\mathcal{M}_\psi$.

$$\widehat{\psi}^2(\text{-}2, \alpha_1) = (\text{-}1, \alpha_1) \text{ and } \widehat{\psi}^2(1, \alpha_2) = (1, \alpha_2^2).$$

From Lemma 3.4.2 this is a well defined map, and is surjective. In general it is not injective. For instance if p, s and t are pairwise coprime positive integers and we have $m_1 = ps$, $m_2 = pt$ and $a = st$, then $d_1 = \gcd(|m_1|, a) = s$, $d_2 = \gcd(|m_2|, a) = t$, $\alpha_1 = a/d_1 = t$ and $\alpha_2 = a/d_2 = s$. If, for some non-trivial $\Lambda \in \langle A \rangle$ we have (m_1, Λ^s) and (m_2, Λ^t) in $\mathcal{M}_\psi$ then both these elements are mapped by $\widehat{\psi}^a$ to (p, Λ^{st}).

Proposition 3.4.7. *Let ψ and φ be regular infinite elements of $G_{2,1}$, let a and b be positive integers and let the images of $\widehat{\psi}^a$ and $\widehat{\varphi}^b$ be*

$$\mathcal{M}_{\psi^a} = \{(p_i, \Gamma_i^{\alpha_i}) | i = 1, \ldots, M\} \text{ and } \mathcal{M}_{\varphi^b} = \{(q_i, \Delta_i^{\beta_i}) | i = 1, \ldots, N\}.$$

For $i = 1, \ldots, M$, let

$$(\widehat{\psi}^a)^{-1}(p_i, \Gamma_i^{\alpha_i}) = \{(m_{i,j}, \Gamma_{i,j}) | 1 \leq j \leq M_i\}$$

and, for $i = 1, \ldots, N$, let

$$(\widehat{\varphi}^b)^{-1}(q_i, \Delta_i^{\beta_i}) = \{(n_{i,j}, \Delta_{i,j}) | 1 \leq j \leq N_i\}.$$

If $\psi^a \sim \varphi^b$ then $M = N$ and, after reordering if necessary, we have $p_i = q_i$ and $\Gamma^{\alpha_i} = \Delta^{\beta_i}$. Moreover, there exist positive integers $\alpha, \beta, d_{i,j}, e_{i,k}, s_{i,j,k}, t_{i,j,k}, f_{i,j,k}$, and $\Lambda_{i,j,k} \in \langle A \rangle$, for $1 \leq i \leq M$, $1 \leq j \leq M_i$ and $1 \leq k \leq N_i$, such that

$$\alpha = d_{i,j} f_{i,j,k} t_{i,j,k} \text{ and } \beta = e_{i,k} f_{i,j,k} s_{i,j,k}, \text{ for all } i, j, k,$$

and

$$\psi^\alpha \sim \varphi^\beta,$$

where $d_{i,j}$ is a positive divisor of $m_{i,j}$, $e_{i,k}$ is a positive divisor of $n_{i,k}$, $\Gamma_{i,j} = \Lambda_{i,j,k}^{s_{i,j,k}}$ and $\Delta_i = \Lambda_{i,j,k}^{t_{i,j,k}}$, and

$$f_{i',j',k'} \left| \left(\prod_{i,j,k} (t_{i,j,k} d_{i,j}) \right) / t_{i',j',k'} d_{i',j'} \right.,$$

for all i', j', k'.

Proof. Assume $\psi^a \sim \varphi^b$, with $a, b > 0$, and that $\rho^{-1} \psi^a \rho = \varphi^b$. From Lemma 3.3.10, $\mathcal{M}_{\psi^a}$ and $\mathcal{M}_{\varphi^b}$ are equal, so $M = N$, and we may order $\mathcal{M}_{\psi^a}$ so that $(p_i, \Gamma_i^{\alpha_i}) = (q_i \Delta_i^{\beta_i})$, so $p_i = q_i$ and $\Gamma_i^{\alpha_i} = \Delta_i^{\beta_i}$. With the notation for $(\widehat{\psi}^a)^{-1}(p_i, \Gamma_i^{\alpha_i})$ and $(\widehat{\varphi}^b)^{-1}(q_i, \Delta_i^{\alpha_i})$ given in the statement of the proposition, let $d_{i,j} = \gcd(a, |m_{i,j}|)$ and $e_{i,k} = \gcd(b, |n_{i,k}|)$, so

$$m_{i,j}/d_{i,j} = p_i = q_i = n_{i,k}/e_{i,k}$$

and let

$$\alpha_{i,j} = a/d_{i,j}, \beta_{i,k} = b/e_{i,k},$$

and

$$\Gamma_{i,j}^{\alpha_{i,j}} = \Gamma_i^{\alpha_i} = \Delta_i^{\beta_i} = \Delta_{i,k}^{\beta_{i,k}},$$

by Definition 3.4.5, for $1 \leq i \leq M$, $1 \leq j \leq M_i$ and $1 \leq k \leq N_i$.

As $\Gamma_{i,j}^{\alpha_{i,j}} = \Delta_{i,k}^{\beta_{i,k}}$, by Proposition 2.4.16, there exist $\Lambda_{i,j,k} \in \langle A \rangle$ and positive integers $s_{i,j,k}, t_{i,j,k}$ such that $\Gamma_{i,j} = \Lambda_{i,j,k}^{s_{i,j,k}}$ and $\Delta_{i,j} = \Lambda_{i,j,k}^{t_{i,j,k}}$. Taking a power of $\Lambda_{i,j,k}$ if necessary, we may assume that $\gcd(s_{i,j,k}, t_{i,j,k}) = 1$. Then

$$\Lambda_{i,j,k}^{s_{i,j,k}\alpha_{i,j}} = \Gamma_{i,j}^{\alpha_{i,j}} = \Delta_{i,k}^{\beta_{i,k}} = \Lambda_{i,j,k}^{t_{i,j,k}\beta_{i,k}},$$

so $s_{i,j,k}\alpha_{i,j} = t_{i,j,k}\beta_{i,k}$. As $s_{i,j,k}$ and $t_{i,j,k}$ are coprime this implies that $\alpha_{i,j}/t_{i,j,k} = \beta_{i,k}/s_{i,j,k} = c_{i,j,k} \in \mathbb{Z}$, and $\alpha_{i,j} = c_{i,j,k} t_{i,j,k}$ and $\beta_{i,k} = c_{i,j,k} s_{i,j,k}$.

Let

$$g = \gcd(\{c_{i,j,k} | 1 \leq i \leq M, 1 \leq j \leq M_i, 1 \leq k \leq N_i\}).$$

Then there exist integers $f_{i,j,k}$ such that $c_{i,j,k} = g f_{i,j,k}$, for all i, j, k. From Lemma 3.4.2,

$\mathcal{M}_{\psi^{a/g}}$ consists of elements $(m/p, \Gamma^{\alpha})$, where $(m, \Gamma) \in \mathcal{M}_{\psi}$, $p = \gcd(m, a/g)$ and $\alpha = a/gp$. Similarly, elements of $\mathcal{M}_{\varphi^{b/g}}$ are of the form $(n/q, \Delta^{\beta})$, where $(n, \Delta) \in \mathcal{M}_{\varphi}$, $q = \gcd(n, b/g)$ and $\beta = b/gq$. Now $g|c_{i,j,k}$ and $c_{i,j,k}|\alpha_{i,j}$ and $c_{i,j,k}|\beta_{i,k}$. Therefore $\gcd(|m_{i,j}|, a/g) = \gcd(|m_{i,j}|, a) = d_{i,j}$ and similarly $\gcd(|n_{i,k}|, b/g) = e_{i,k}$. Thus g is coprime to

$$p_i = \frac{m_{i,j}}{\gcd(|m_{i,j}|, a/g)} = \frac{n_{i,k}}{\gcd(|n_{i,k}|, b/g)},$$

for all i, j, k. From Lemma 3.4.4, it follows that $\psi^{a/g} \sim \varphi^{b/g}$.

Now

$$a/g = \alpha_{i,j} d_{i,j}/g = c_{i,j,k} t_{i,j,k} d_{i,j}/g = f_{i,j,k} t_{i,j,k} d_{i,j}$$

and similarly

$$b/g = f_{i,j,k} s_{i,j,k} e_{i,k},$$

for all i, j, k. Also

$$\gcd(\{f_{i,j,k} | 1 \leq i \leq M, 1 \leq j \leq M_i, 1 \leq k \leq N_i\}) = 1$$

so, for fixed i', j', k',

$$f_{i',j',k'} \left| \left(\prod_{i,j,k} (t_{i,j,k} d_{i,j}) \right) / t_{i',j',k'} d_{i',j'} \right.$$

□

Corollary 3.4.8. *The power conjugacy problem for regular infinite elements of $G_{2,1}$ is solvable.*

Proof. Let ψ and φ be regular infinite elements of $G_{2,1}$. Suppose that ψ^a is conjugate to φ^b, for some non-zero a, b. Replacing either ψ or φ or both by their inverse, we may assume that $a, b > 0$. Then, in the notation of the proposition above, we have $\psi^{\alpha} \sim \varphi^{\beta}$, where $\alpha = f_{i,j,k} t_{i,j,k} d_{i,j}$ and $\beta = f_{i,j,k} s_{i,j,k} e_{i,k}$. From the conclusion of the theorem it is clear that there are finitely many choices for $f_{i,j,k}$, $s_{i,j,k}$, $t_{i,j,k}$, $d_{i,j}$ and $e_{i,k}$. Hence there are finitely many possible α and β, and we may effectively construct a list of all possible pairs (α, β). Having constructed this list we may check whether or not $\psi^{\alpha} \sim \varphi^{\beta}$, using Algorithm 3.3.25 Step 3. Hence we may decide whether or not there exist a, b such that $\psi^a \sim \varphi^b$. □

Example 3.4.9. Let ψ be a regular infinite element of $G_{2,1}$ in quasi-normal form with respect to

$$X = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\}$$

and defined by a bijective map with

$$U = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\}$$

given by $x\alpha_1^2\psi = x\alpha_1$, $x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1$ and $x\alpha_2\psi = x\alpha_2^2$.

Let φ be a regular infinite element of $G_{2,1}$ in quasi-normal form with respect to

$$Y = \{x\alpha_1, x\alpha_2\alpha_1^3, x\alpha_2\alpha_1^2\alpha_2, x\alpha_2\alpha_1\alpha_2, x\alpha_2^2\}$$

and defined by a bijective map with

$$V = \{x\alpha_1^2, x\alpha_1\alpha_2\alpha_1, x\alpha_1\alpha_2^2\alpha_1, x\alpha_1\alpha_2^3, x\alpha_2\}$$

given by $x\alpha_1\varphi = x\alpha_1\alpha_2^3$, $x\alpha_2\alpha_1^3\varphi = x\alpha_2$, $x\alpha_2\alpha_1^2\alpha_2\varphi = x\alpha_1^2$, $x\alpha_2\alpha_1\alpha_2\varphi = x\alpha_1\alpha_2\alpha_1$ and $x\alpha_2^2\varphi = x\alpha_1\alpha_2^2\alpha_1$.

Then $\mathcal{M}_\psi = \{(1, \alpha_2), (\text{-}1, \alpha_1)\}$ and $\mathcal{M}_\varphi = \{(1, \alpha_2^3), (\text{-}1, \alpha_1^3)\}$. Assume there exists positive integers a, b such that $\psi^a \sim \varphi^b$. Therefore, by Proposition 3.4.7 we can define

$$\mathcal{M}_{\psi^a} = \{(p_i, \Gamma_i^{\alpha_i}) : i = 1, \ldots, M\} \text{ and } \mathcal{M}_{\varphi^b} = \{(q_i, \Delta_i^{\beta_i}) : i = 1, \ldots, N\}.$$

We have the map $\widehat{\psi}^a : \mathcal{M}_\psi \to \mathcal{M}_{\psi^a}$,

$$\widehat{\psi}^a(1, \alpha_2) = (1/d_1, \alpha_2^{a/d_1})$$

$$\widehat{\psi}^a(\text{-}1, \alpha_1) = (\text{-}1/d_2, \alpha_1^{a/d_2})$$

where $d_1 = \gcd(1, a) = 1$ and $d_2 = \gcd(|\text{-}1|, a) = 1$. Thus, we can write,

$$\mathcal{M}_{\psi^a} = \{(1, \alpha^a), (\text{-}1, \alpha_1^a)\}.$$

We have the map $\widehat{\varphi}^b : \mathcal{M}_\varphi \to \mathcal{M}_{\varphi^b}$,

$$\widehat{\varphi}^b(1, \alpha_2) = (1/d_1, \alpha_2^{3b/d_1})$$

$$\widehat{\varphi}^b(\text{-}1, \alpha_1) = (\text{-}1/d_2, \alpha_1^{3b/d_2})$$

where $d_1 = \gcd(1, b) = 1$ and $d_2 = \gcd(|\text{-}1|, b) = 1$. Thus, we can write,

$$\mathcal{M}_{\varphi^b} = \{(1, \alpha^{3b}), (\text{-}1, \alpha_1^{3b})\}.$$

By Proposition 3.4.7 we require the integers a, b to satisfy $a = 3b$. The smallest possibility for (a, b) is $(3, 1)$. We can now apply Step 3 from Algorithm 3.3.25 for ψ^3, φ to determine if they are conjugate.

We find a conjugating element ρ, given by $x\alpha_1\rho = x\alpha_2$ and $x\alpha_2\rho = x\alpha_1$.

Example 3.4.10. Let ψ be from Example 3.4.3. Let φ be a regular infinite element of $G_{2,1}$ in quasi-normal form with respect to

$$X = \{x\alpha_1^2, x\alpha_1\alpha_2, x\alpha_2\}$$

and defined by a bijective map with

$$U = \{x\alpha_1, x\alpha_2\alpha_1, x\alpha_2^2\}$$

given by $x\alpha_1^2\psi = x\alpha_1$, $x\alpha_1\alpha_2\psi = x\alpha_2\alpha_1$ and $x\alpha_2\psi = x\alpha_2^2$.

Then $\mathcal{M}_\psi = \{(\text{-}2, \alpha_1), (1, \alpha_2)\}$ and $\mathcal{M}_\varphi = \{(1, \alpha_2), (\text{-}1, \alpha_1)\}$. Assume there exists positive integers a, b such that $\psi^a \sim \varphi^b$. Therefore, by Proposition 3.4.7 we can define

$$\mathcal{M}_{\psi^a} = \{(p_i, \Gamma_i^{\alpha_i}) : i = 1, \ldots, M\} \text{ and } \mathcal{M}_{\varphi^b} = \{(q_i, \Delta_i^{\beta_i}) : i = 1, \ldots, N\}.$$

We have the map $\widehat{\psi}^a : \mathcal{M}_\psi \to \mathcal{M}_{\psi^a}$,

$$\widehat{\psi}^a(1, \alpha_2) = (1/d_1, \alpha_2^{a/d_1})$$

$$\widehat{\psi}^a(\text{-}2, \alpha_1) = (\text{-}2/d_2, \alpha_1^{a/d_2})$$

where $d_1 = \gcd(1, a) = 1$ and $d_2 = \gcd(|\text{-}2|, 1) = 1$ or 2. Thus, we can write,

$$\mathcal{M}_{\psi^a} = \{(1, \alpha^a), (\text{-}2, \alpha_1^a)\} \text{ or } \{(1, \alpha^a), (\text{-}1, \alpha_1^{a/2})\}.$$

We have the map $\widehat{\varphi}^b : \mathcal{M}_\varphi \to \mathcal{M}_{\varphi^b}$,

$$\widehat{\varphi}^b(1, \alpha_2) = (1/d_1, \alpha_2^{b/d_1})$$

$$\widehat{\varphi}^b(\text{-}1, \alpha_1) = (\text{-}1/d_2, \alpha_1^{b/d_2})$$

where $d_1 = \gcd(1, b) = 1$ and $d_2 = \gcd(|\text{-}1|, b) = 1$. Thus, we can write,

$$\mathcal{M}_{\varphi^b} = \{(1, \alpha^b), (\text{-}1, \alpha_1^b)\}.$$

By Proposition 3.4.7, we require that $\mathcal{M}_{\psi^a} = \mathcal{M}_{\varphi^b}$. Therefore,

$$\mathcal{M}_{\psi^a} = \{(1, \alpha^a), (\text{-}1, \alpha_1^{a/2})\}.$$

This implies that $b = a/2$ and $b = a$. Thus, there do not exist integers $a, b > 0$ such that ψ^a is conjugate to ψ^b by Proposition 3.4.7. The same argument applies replacing

ψ or φ by ψ^{-1} or φ^{-1} respectively, so no nontrivial power of ψ is conjugate to a power of φ.

Algorithm 3.4.11. Let ψ and φ be regular infinite elements in quasi-normal form with respect to the basis X and Y.

Step 1: Construct the sets $\mathcal{M}_\psi$ and $\mathcal{M}_\varphi$ (see Definition 3.3.8).

Step 2: Calculate the bounds on $a_{\max}$ and $b_{\max}$ as in Corollary 3.4.8.

Step 3: For all a, b such that $0 < a \leq a_{\max}$ and $0 < b \leq b_{\max}$ apply the remaining steps of the algorithm to ψ and φ, and to ψ^{-1} and φ.

Step 4: Calculate the sets $\mathcal{M}_{\psi^a}$ and $\mathcal{M}_{\varphi^b}$ using the maps $\widehat{\psi}^a : \mathcal{M}_\psi \to \mathcal{M}_{\psi^a}$ and $\widehat{\varphi}^b : \mathcal{M}_\varphi \to \mathcal{M}_{\varphi^b}$ (see Definition 3.4.5).

Step 5: For each pair (a, b) such that $\mathcal{M}_{\psi^a} = \mathcal{M}_{\varphi^b}$ apply Step 4 of Algorithm 3.3.25 to the elements ψ^a and φ^b to check for conjugacy.

We define the set $\mathcal{PC}_{RI}$ of all the pairs (a, b) that satisfy the condition that ψ^a is conjugate to φ^b, and $0 < a \leq a_{\max}$ and $0 < b \leq b_{\max}$.

3.4.2 Power Conjugacy Algorithm

Algorithm 3.4.12. Let ψ and φ be elements in quasi-normal form with respect to the basis X and Y.

Step 1: By Theorem 3.1.1, we split the elements ψ and φ into their periodic parts ψ_P, φ_P and their regular infinite parts ψ_{RI}, φ_{RI}.

Step 2: For ψ_{RI} and ψ_P use Algorithm 3.1.6 to construct isomorphisms f_{RI}, f_P and regular infinite element $\widehat{\psi_{RI}} = f_{RI}^{-1}\psi_{RI}f_{RI}$ and periodic element $\widehat{\psi_{RI}} = f_P^{-1}\psi_P f_P$. Similarly, use Algorithm 3.1.6 to construct isomorphisms g_{RI}, g_P and regular infinite element $\widehat{\varphi_{RI}} = g_{RI}^{-1}\varphi_{RI}g_{RI}$ and periodic element $\widehat{\varphi_{RI}} = g_P^{-1}\varphi_P g_P$.

Step 3: To the elements $\widehat{\psi_P}$, $\widehat{\varphi_P}$ of $G_{2,1}$ we work through Section 3.4.1 to give the set $\mathcal{PC}_P$;

Step 4: To the elements $\widehat{\psi_{RI}}$, $\widehat{\varphi_{RI}}$ of $G_{2,1}$ we work through Algorithm 3.4.11 to give the set $\mathcal{PC}_{RI}$;

Step 5: We combine Step's 3 and 4. If $\mathcal{PC}_P$ or $\mathcal{PC}_{RI}$ is empty then there is no non-trivial power of ψ that is conjugate to a non-trivial power of φ. Otherwise, choose a pair (a_{RI}, b_{RI}) in $\mathcal{PC}_{RI}$ and a pair (a_P, b_P) in $\mathcal{PC}_P$ and define (a', b') by $a' = ka_P$ and $b' = kb_P$ for $k, l \in \mathbb{Z} \setminus \{0\}$ such that the pair k, l is a solution to the simultaneous equations $ka_p = la_{RI}$, $kb_p = lb_{RI}$. Then $\psi^{a'} \sim \varphi^{b'}$.

Note that, following this algorithm through produces a conjugating element from $\psi^{a'}$ to $\varphi^{b'}$ if such a pair (a', b') exists.

Theorem 3.4.13. *The power conjugacy problem for the Higman-Thompson group $G_{2,1}$ is solvable.*

Proof. Apply Algorithm 3.4.12. □

Part II

Beauville p-groups

Chapter 4

Introduction

Chapter 5 comprises work conducted under the supervision of Nigel Boston, Norbert Peyerimhoff and Alina Vdovina. The work in Chapter 5 is published [BBPV11a].

The work presented in Chapter 6 comprises work conducted under the supervision of Nigel Boston and Ben Fairbairn. This work has been published, [BBF12].

This part of the thesis is concerned with ramification structures coming from finite groups which give rise to certain algebraic surfaces of general type known as Beauville surfaces.

Aims of Work Part II

We begin this part of the thesis with a brief introduction into the motivation for the work in Chapters 5 and 6 from algebraic geometry. We make no attempt to define all the terms but give a rough outline of the progression of the work in the field in order to put Chapters 5 and 6 in context. References to the literature for the interested reader are given throughout.

It is a fundamental fact that a complex algebraic curve of genus zero is isomorphic to the complex projective line $\mathbb{P}^1$.

The search for an similar statement by algebraic geometers in the case of algebraic surfaces led Max Noether to conjecture that a smooth regular (*i.e.* irregularity of a surface S, $q(S) = 0$) algebraic surface with vanishing geometric genus ($P_g(S) = 0$) should be a rational surface (see [Bea96, Mir95],).

The first counterexample to this conjecture was provided by Federgo Enriques in 1896 (see [Enr1896]). This was followed in the 1930s by Lugi Campedelli and Lucian Godeaux (see [Cam32, Go35]) who constructed more counterexamples to the above conjecture. These surfaces now form part of the study of algebraic geometry know as surfaces of general type (see [Bea96, Mir95]).

In the 1970s, many new examples were found, this time the construction of these

new surfaces came via quotients $S = Z/G$ of simpler (better understood) surfaces Z by a free action of a finite group G.

Definition 4.0.14 (Free Action)**.** Let G be a group and X a topological space. A group action $G \times X \to X$ is called free if for all $x \in X$, $gx = x$ for $g \in G$ if and only if $g = Id_G$.

In 1978, Arnaud Beauville [Bea78] produced a construction by taking Z to be the direct product of two curves $\mathcal{C}_1$ and $\mathcal{C}_2$ of genera $g_1 := g(\mathcal{C}_1)$ and $g_2 := g(\mathcal{C}_2)$ respectively, together with an action of a group G of order $(g_1 - 1)(g_2 - 1)$.

Remark 4.0.15. This method produces surfaces with self-intersection number of a canonical divisor for the surface $K^2 = 8$.

Beauville also gave an explicit example as a quotient of two Fermat curves, see Section 4.1 for more details.

In [Bea78], Beauville's construction of these particular type of surfaces was generalized to what is now known as surfaces isogenous to a product of curves. That is, surfaces which have a finite unramified cover which is biholomorphic to a product of two curves.

Definition 4.0.16. A surface S is isogenous to a higher product if both curves have genus greater than or equal to 2.

Remark 4.0.17. If S is a surface isogenous to a higher product, then S is a surface of general type (see [Bea96]).

As a consequence of several results in complex algebraic geometry (see [Cat00]) any surface S isogenous to a higher product has a unique minimal realisation $S \cong (\mathcal{C}_1 \times \mathcal{C}_2)/G$ where G is a finite group acting freely on the direct product $\mathcal{C}_1 \times \mathcal{C}_2$ with $g_1, g_2 \geq 2$ chosen as small as possible.

However, we take advantage of the work from [BCG05, BCG06, BCG08] which translates the technical details from complex algebraic geometry for S to be isogenous to a higher product to conditions on the finite group G which acts freely on the product of the two curves $\mathcal{C}_1 \times \mathcal{C}_2$, with $|G| = (g_1 - 1)(g_2 - 1)$. We state the conditions on the finite group G in Chapter 5, where the definitions are introduced more formally.

It was, therefore, the work of [BCG05, BCG06, BCG08] which motivates the work of Chapter 5, where the following results are achieved.

We find ramification structures for finite groups constructed as 2-quotients of a particular infinite group with "special presentation" related to the finite projective plane of order 2 and which is also the fundamental group of the one skeleton of the CW-complex of an $\widetilde{A}_2$ building.

The ramification structures obtained give rise to specific surfaces of general type, Beauville surfaces. We find new mixed and unmixed Beauville surfaces coming from Beauville structures constructed from 2-quotients of 2-power order of the fundamental group of a certain simplicial complex, in Chapter 5. With the terms defined in due course, the following theorems are obtained. First, a theorem which provides a number of *unmixed Beauville surfaces*.

Theorem 5.3.1: Let $3 \leq k \leq 63$, $r = \lfloor \log_2 k \rfloor + 1$ and $A = [2^r, 2^r, 2^r]$. If k is not a power of 2, then (T_1, T_2) is an *unmixed Beauville structure* of type (A, A) for the group $H_{2,k}$.

Secondly, a theorem which can be used to create a number of *mixed Beauville surfaces*.

Theorem 5.3.2: Let $3 \leq k \leq 10$ and $r = \lfloor \log_2 k \rfloor + 1$. If k is not a power of 2, then $(H_{2,k}, T_1)$ is a *mixed Beauville structure* of type $[2^r, 2^r, 2^r]$ for the group $G_{2,k}$.

Mixed Beauville surfaces are known to be rare and creation of new examples are welcome in the field of algebraic geometry, we will say more on this in Chapter 5.

We finish with Chapter 6 which examines current progress on the existence and classification of non-abelian Beauville p-groups. With the terms defined in due course, the following theorems and corollaries are obtained.

An examination of group presentations for 2-generator p-groups of order p^5 leads to the first theorem and corollary.

Theorem 6.0.1: If $p > 3$, then there exists at least $p + 8$ Beauville groups of order p^5.

Corollary 6.0.2: The proportion of 2-generated groups of order p^5 that are Beauville tends to 1 as p tends to infinity.

An examination of group presentations for 2-generator p-groups of order p^6 leads to the second theorem and corollary on this subject.

Theorem 6.0.3: If $p > 3$, then there exist at least $p - 1$, 2-generated non-Beauville groups of order p^6.

Corollary 6.0.4: The proportion of 2-generated groups of order p^6 that are Beauville does not tend to 1 as p tends to infinity.

Throughout Chapter 6, computer calculations using the computer algebra program MAGMA (and computer scripts written by the author of this thesis) gives rise to the following corollary.

Corollary 6.0.6: The smallest non-abelian Beauville p-groups are

1. for $p = 2$, `SmallGroup`(2^7,36);

2. for $p = 3$, the group given by Example 6.4.1, of order 3^5;

3. for $p = 5$, `SmallGroup`(5^3,3);

4. for $p \geq 7$, the groups given by Lemma 6.2.1, of order p^3.

The work of Chapter 6 provides more information to address the following question, [BCG06, Question 7.7a]: *"Classification of Beauville surfaces: which finite groups can occur?"*

In addition, it is also the beginnings of a line of work which should address a statement which was made in the work of [FGZ10] "it is very plausible that most 2-generated finite p-groups of sufficiently large order [are Beauville groups]". Hence, it was the work of [FGZ10] and [BCG06] which motivates the work of Chapter 6.

Notation

We will write $\mathbb{P}^1$ for the Riemann sphere (complex projective line), $Sym(n)$ for the symmetric group of order $n!$ and $\mathbb{Z}_n$ for the integers modulo n.

4.1 Beauville surfaces

In recent years a number of people have been interested in the study of Beauville surfaces and finite groups (see, e.g., [FJ09], [GP09b], [BCG10], [Gar10], [GLL10], [FG10] and [FGZ10]).

From [Cat00, Definition 3.23], a Beauville surface S is an infinitesimally rigid (i.e., does not admit non-trivial deformations) complex regular algebraic surface, which is *isogenous to a higher product*. This means that S is of the form $(\mathcal{C}_1 \times \mathcal{C}_2)/G$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are non-singular projective curves of genera $g(\mathcal{C}_i) \geq 2$, and G is a finite group acting freely on the product of curves by holomorphic transformations.

Let H denote the subgroup of G consisting of the elements of G which preserve each of the curves $\mathcal{C}_i$. The presentation $S \cong (\mathcal{C}_1 \times \mathcal{C}_2)/G$ is called *minimal* if H acts freely on each curve $\mathcal{C}_i$ (*i.e.* the only element of H that fixes every point on each $\mathcal{C}_i$ is the identity element).

Every Beauville surface S has a unique minimal presentation $(\mathcal{C}_1 \times \mathcal{C}_2)/G$. Moreover, the corresponding quotients $\mathcal{C}_i/H$ are isomorphic to $\mathbb{P}^1$, and the projections $\mathcal{C}_i \to \mathbb{P}^1$ are branched coverings, ramified over three points. These properties are equivalent to the rigidity of Beauville surfaces, which means that Beauville surfaces represent isolated points in the moduli space of surfaces of general type (see [Bea96] for a definition of moduli space of surfaces of general type).

A Beauville surface $(\mathcal{C}_1 \times \mathcal{C}_2)/G$ is said to be of *mixed* or *unmixed* type, according to whether $[G : H] = 2$ (i.e., G contains elements interchanging the curves $\mathcal{C}_1$ and $\mathcal{C}_2$) or $H = G$, and the group G is said to admit a mixed or unmixed Beauville structure, respectively (we make formal definitions of mixed and unmixed Beauville structure for a finite group G in Chapter 5). In the mixed case, the curves $\mathcal{C}_1$ and $\mathcal{C}_2$ are necessarily biholomorphic.

Beauville's original example [Bea78] had two curves $\mathcal{C}_1 = \mathcal{C}_2$, given by the Fermat curve $x^5 + y^5 + z^5 = 0$, and G the group $\mathbb{Z}_5 \times \mathbb{Z}_5$ acting on $\mathcal{C}_1 \times \mathcal{C}_2$ by the rule

$$(a, b) \cdot ([x : y : z], [u : v : w]) = ([\xi^a x : \xi^b y : z], [\xi^{a+3b} u : \xi^{2a+4b} v : w]),$$

where $\xi = e^{\frac{2\pi i}{5}}$ and $a, b \in \mathbb{Z}_5$. Then S is a Beauville surface of unmixed type with $g(\mathcal{C}_1) = g(\mathcal{C}_2) = 6$.

Most of what is known about Beauville surfaces is due to the work of Catanese in [Cat00] and the joint work of Bauer, Catanese and Grunewald in [BCG05, BCG06] and [BCG08]. However, not many examples of Beauville surfaces of mixed type are known.

Bauer, Catanese and Grunewald [BCG05, BCG06] showed that all sufficiently large alternating groups admit an unmixed Beauville structure, and conjectured that all finite (non-abelian) simple groups, except A_5, admit such a structure. This conjecture was first been proved for the alternating groups A_n ($n > 5$) in [FG10], and then for the groups $PSL(2, q)$ ($q \geq 7$) as well as some other families of finite simple groups of Lie type with low Lie rank in [FJ09, GP09a]. In 2010/2011 the full conjecture was shown to be true.

Theorem 4.1.1. *[GLL10, GM10, FMP10] All finite (non-abelian) simple groups, except A_5, admit a Beauville structure.*

In addition, the symmetric groups $Sym(n)$ ($n > 4$) and all finite quasisimple groups (except $SL(2, 5)$ and $PSL(2, 5) \cong A_5$) admit unmixed Beauville structures by [FG10, FJ09, FMP10].

Remark 4.1.2. A finite group is called *quasisimple* if it is isomorphic to its commutator subgroup and its inner automorphism group is a simple group.

Let G be a finite group. We call G a *Beauville group* if there exists a 'Beauville structure' for G, which we define in Chapter 5, Definition 5.1.7.

In [BCG06, Question 7.7] Bauer, Catanese and Grunewald ask which groups are Beauville groups and, given a Beauville group, what are its Beauville structures? In [Cat00] Catanese classified the abelian Beauville groups by proving the following.

Theorem 4.1.3. *[Cat00, Lemma 3.21 & Beauville's examples 3.22] G is an abelian Beauville group if and only if $G = \mathbb{Z}_n \times \mathbb{Z}_n$ where $\mathbb{Z}_n$ is the cyclic group of order n and $gcd(n, 6) = 1$.*

After Abelian groups, the next most natural class to consider are the nilpotent groups. Recalling that a finite group is nilpotent if and only if it is a direct product of its Sylow subgroups (see Section 4.2), Lemma 6.1.1 of Chapter 6 reduces the study of nilpotent Beauville groups to the study of Beauville p-groups, which is the case we focus on in Chapter 6.

Notice that Theorem 4.1.3 gives us an infinite supply of Beauville p-groups for every $p \geq 5$ - simply let n be a power of p. Various examples of non-abelian Beauville p-groups for specific values of p have appeared elsewhere [BBPV11a, BBPV11b, FGZ10], but little has been said about the general case until [BBF12] and Chapter 6.

4.2 Finite groups of prime power order

We now state some important information from the world of finite p-groups.

Let p be a prime number. A finite group G is called a p-group if its order $|G|$ is a power of a prime p.

Theorem 4.2.1 (Lagrange's Theorem)**.** *[Rob96, Theorem 1.3.6] If G is a group and H is a subgroup of G, then $|G| = |G : H| \cdot |H|$. If G is finite, $|G : H| = |G|/|H|$. Hence the order of a subgroup always divides the order of the group if the latter is finite.*

By Lagrange's Theorem, the order of each element of a p-group must also be a power of p.

It was first proved by Sylow [Syl1872], that every group of prime power order p^n has a presentation of the form,

$$\langle a_1, ..., a_n | a_i^p = v_{i,i}, 1 \leq i \leq n, [a_k, a_j] = v_{j,k}, 1 \leq j < k \leq n \rangle,$$

where the $v_{j,k}$ are words in the elements $a_{k+1}, ..., a_n$ for $1 \leq j < k \leq n$. A presentation of this form is called (these days) a *power-commutator* presentation for the group. It is standard, in order to save space, to omit relations of the form $[a_k, a_j] = e$ in the presentation.

If $|G| = p^a m$ where $\gcd(p, m) = 1$, then a p-subgroup of G cannot have order greater than p^a by Lagrange's Theorem. A p-subgroup of G which has this maximum order p^a is called a *Sylow p-subgroup* of G.

Sylow p-subgroups of G always exist and any two are conjugate.

Theorem 4.2.2 (Sylow's Theorem)**.** *[Rob96, Theorem 1.6.16] Let G be a finite group and p a prime. Write $|G| = p^a m$ where the integer m is not divisible by p.*

1. *Every p-subgroup of G is contained in a subgroup of order p^a.*
2. *If n_p is the number of Sylow p-subgroups, $n_p \equiv 1 \mod p$.*

3. *All the Sylow p-subgroups are conjugate in G.*

We now state some general definitions about certain families of subgroups that can be formed from a group G.

Definition 4.2.3. [L-GM02, Definition 1.1.10] A family of subgroups $G_0, G_1, ...$ of G forms a descending series in G if

$$G = G_0 \geq G_1 \geq G_2 \geq ...,$$

and $G_i + 1 \lhd G_i$ for all $i \geq 0$. The sections of this series are the quotients G_i/G_{i+1}.

Similarly, the family of subgroups $G_0, G_1, ...$ of G forms an ascending series in G if

$$\langle e \rangle = G_0 \leq G_1 \leq G_2 \leq ...,$$

and $G_i \lhd G_i + 1$ for all $i \geq 0$. The sections of this series are the quotients G_{i+1}/G_i.

An ascending or descending series, as above, is a normal series if $G_i \lhd G$ for all $i \geq 1$; it is a central series if it is a normal series such that G centralizes every section; and it is finite if $G_i = G_{i+1}$ for all but finitely many values of i. In a finite group a composition series is a series in which every section is simple.

In a finite group, a descending chief series is a normal series

$$G = G_0 > G_1 > ... > G_n = \langle e \rangle$$

such that for every i there is no normal subgroup N of G such that $G_{i+1} < N < G_i$. An ascending chief series is defined similarly.

Definition 4.2.4. [L-GM02, Definition 1.1.13] The upper central series of G is the series

$$\langle e \rangle = \zeta_0(G) \leq \zeta_1(G) \leq \zeta_2(G) \leq ...,$$

of subgroups of G defined inductively by $\zeta_i(G)/\zeta_{i-1}(G) = Z(G/\zeta_{i-1}(G))$ for $i > 0$.

G is nilpotent if there exists an integer k such that $\zeta_k(G) = G$.

If G is nilpotent, the nilpotentcy class c of G is the smallest integer $c \geq 1$ such that $\zeta_c(G) = G$.

We can finally state the following theorem.

Theorem 4.2.5. *[Rob96, Theorem 5.2.4] Let G be a finite group. Then the following properties are equivalent:*

1. *G is nilpotent;*

2. *G is the direct product of its Sylow subgroups.*

4.3 The pQuotient algorithm

We will often refer to the computer programs GAP and MAGMA, specifically to the function `pQuotient`.

The algorithm `pQuotient` (see [BCP97]) uses the lower exponent p-central series, that is a descending sequence of subgroups

$$G = P_0(G) \geq ... \geq P_{i-1}(G) \geq P_i(G) \geq ...,$$

where $P_i(G) = [P_{i-1}(G), G]P_{i-1}(G)^p$ for $i \geq 1$. The p-class k of G is the length of the series. The algorithm constructs a consistent power-conjugate presentation for the largest p-quotient of G of p-class k

We thus obtain results on ramification structures of finite groups obtained from particular groups G with special representations. These finite groups are generated via the lower exponent p-central series. The finite groups $G_{p,k}$ under considerations in Chapter 5 are then the maximal p-quotients of p-class k, denoted by $G_{p,k}$ and given by $G_{p,k} = G/P_k(G)$.

4.4 The Small Groups Library

We will reference the MAGMA and GAP database know as the `SmallGroup` library, [SmallGroups].

For the creation of the Small Groups library, Hans Ulrich Besche, Bettina Eick and Eamonn O'Brien developed practical algorithms to construct the groups of a given order. A survey of the construction of the library can be found here [BBO02].

The library contains all groups of "small" order, up to isomorphism. More specifically:

- groups of order at most 2000 except 1024 (423164062 groups);
- groups of cubefree order at most 50000 (395703 groups);
- groups of order p^7 for the primes $p = 3, 5, 7, 11$ (907489 groups);
- groups of order p^n for $n \leq 6$ and all primes p;
- groups of order $q^n p$ where q^n divides 28, 36, 55 or 74 and p is an arbitrary prime not equal to q;
- groups of square-free order;
- groups whose order factorises into at most 3 primes.

The library also has an identification function which returns the library number of a given group. Currently, this function is available for all orders in the library except for the orders 512 and 1536 and except for the orders p^5, p^6 and p^7 above 2000.

Chapter 5

Mixed and Unmixed Beauville Surfaces

We will first introduce the contents of the chapter. Let

$$\Gamma = \langle x_0, ..., x_6 \mid x_i x_{i+1} x_{i+3} \text{ for } i = 0, ..., 6 \rangle,$$

and H be the index 2 subgroup generated by x_0, x_1 (see Proposition 5.2.1). Moreover, let $G_{2,k}$ and $H_{2,k}$ denote the maximal 2-quotients of 2-class k (see Section 4.3 for the precise definition) of Γ and H, respectively (for more details see Sections 5.2 and 5.3 below). We find that $H_{2,k}$ has an *unmixed Beauville structure* for every $3 \leq k \leq 63$ which is not a power of 2 (see Theorem 5.3.1), and that $G_{2,k}$ admits a *mixed Beauville structure* for every $3 \leq k \leq 10$ which is not a power of 2 (see Theorem 5.3.2). We conjectured in [BBPV11a] that both results hold generally for all 2-classes $k \geq 3$ which are not powers of 2. This would provide infinitely many 2-groups admitting unmixed (or mixed) Beauville structures.

5.1 Beauville surfaces

Inspired by a construction of Beauville, Catanese defined in [Cat00] a *Beauville surface* to be a rigid (i.e., it admits no nontrivial deformation) compact complex surface which is isogeneous to a higher product, i.e., it admits an unramified covering which is isomorphic to a product of curves of genera ≥ 2.

It was shown in [Cat00] that every such surface has a unique minimal realisation $S := (\mathcal{C}_1 \times \mathcal{C}_2)/G$, such that the genera of the curves $\mathcal{C}_1$ and $\mathcal{C}_2$ are minimal. Moreover, in a minimal realization the action of G on $\mathcal{C}_1 \times \mathcal{C}_2$ is free and respects the product decomposition, i.e., the elements of G either interchange the factors or act independently on both factors. This allows us to distinguish two types of Beauville

surface (as mentioned in Chapter 4), which we now formally define:

Definition 5.1.1. Let S be a surface isogenous to a product of curves with minimal realisation $S \cong (\mathcal{C}_1 \times \mathcal{C}_2)/G$. We say that S is a *mixed case* if the action of G exchanges the two factors (and then $\mathcal{C}_1$ and $\mathcal{C}_2$ are isomorphic) and an *unmixed case* if G acts via a diagonal action.

Definition 5.1.2. A group G is said to act diagonally on a product of two curves $\mathcal{C}_1 \times \mathcal{C}_2$ if $\forall g \in G$ and $x \in \mathcal{C}_1, y \in \mathcal{C}_2$,

$$g \circ (x, y) = (g \circ x, g \circ y).$$

The definition of Beauville surfaces allows a purely group theoretic intrinsic description of all groups producing them. This collection of group theoretical properties is called a *Beauville structure*, and in the introduction (Chapter 4) it is discussed and in [BCG05] how a group G with a Beauville structure gives rise to a corresponding Beauville surface with minimal realisation $(\mathcal{C}_1 \times \mathcal{C}_2)/G$. As in the case of Beauville surfaces, there are a mixed and unmixed Beauville structures.

Bauer, Catanese and Grunewald [BCG08] used this group theoretical description to classify all smooth complex projective surfaces S isogenous to a product, which are regular, i.e., $q(S) = h^{1,0}(S) = 0$, and which have vanishing geometric genus $p_g(S) = h^{2,0}(S) = 0$. Since a surface S isogeneous to a higher product is of general type, $p_g(S) = 0$ implies $q = 0$, because of $\chi(S) = 1 + p_g(S) - q(S) \geq 1$. Furthermore, Beauville surfaces with $p_g(S) \geq 1$ have also vanishing irregularity $q(S) = 0$, since $q(S) = g(\mathcal{C}_1/H) + g(\mathcal{C}_2/H)$ (see [Ser96, Proposition 2.2]) and $\mathcal{C}_1/H \cong \mathcal{C}_2/H \cong \mathbb{P}^1$.

It turns out that one of the groups in the classification of [BCG08], which they call $G(256, 2)$ and which has a mixed Beauville structure, coincides with the maximal 2-quotient of 2-class 3 of a fundamental group Γ of a certain simplicial complex, which we define in Section 5.2 below. More details about mixed Beauville structures for this group are discussed in Section 5.2.2.

As mentioned in the introduction, not many examples of Beauville surfaces of mixed type are known. It was shown in [BCG05, Theorem 4.3], that if G admits a mixed Beauville structure, then the index 2 subgroup H must be non-abelian, and it was mentioned in [BCG08, Remark 4.2] that no group of order < 256 admits a mixed Beauville structure. Moreover, the classification in [BCG08] implies that there are only two groups occurring in minimal realisations $S \cong (\mathcal{C}_1 \times \mathcal{C}_2)/G$ with $p_g(S) = q(S) = 0$ admitting mixed Beauville structures, and both of them are of order 256.

Our main aim in the subsequent sections below is to show that not only the group $G(256, 2)$ in [BCG08], but also many other maximal 2-quotients of our group Γ produce Beauville surfaces of mixed type. Since their orders are higher 2-powers

than $256 = 2^8$, these other surfaces must necessarily have $p_g(S) \geq 1$.

Remark 5.1.3. It is interesting to note that, by [FG10, Lemma 5], if a group G admits a mixed Beauville structure (H, T) then the order of any element $g \in G \setminus H$ is divisible by 4. Hence, the only p-groups that can admit a mixed Beauville structure are 2-groups. However in the unmixed case, by [BCG05] and [FGZ10], for every prime number p there exists a p-group admitting an unmixed Beauville structure.

5.1.1 Group theoretical structures

Following [BCG08] closely, we introduce group theoretic notions which lead to the definition of Beauville structures.

Let G be a finite group and r an integer with $r \geq 2$. An r-tuple $T = (g_1, ..., g_r)$ of elements of G is called a *spherical system of generators*, if $g_1, ..., g_r$ generate G and we additionally have $g_1 ... g_r = 1$.

Remark 5.1.4. Traditionally, a spherical system of generators is denoted by square brackets however, here we use different parentheses to distinguish them from commutators.

For an r-tuple $T = (g_1, ..., g_r)$ of elements of G and $g \in G$, we set

$$gTg^{-1} := (gg_1g^{-1}, ..., gg_rg^{-1}).$$

If $A = [m_1, ..., m_r]$ is an r-tuple of natural numbers with $2 \leq m_1 \leq ... \leq m_r$, then the spherical system of generators $T = (g_1, ..., g_r)$ is said to be *of type* A, if there is a permutation $\tau \in Sym(r)$ such that we have

$$ord(g_1) = m_{\tau(1)}, ord(g_2) = m_{\tau(2)}, \cdots, ord(g_r) = m_{\tau(r)}.$$

(Here $ord(g)$ is the order of the element $g \in G$.)

For a spherical system of generators $T = (g_1, ..., g_r)$ of G, we define

$$\Sigma(T) = \Sigma((g_1, ..., g_r)) := \bigcup_{g \in G} \bigcup_{j=0}^{\infty} \bigcup_{i=1}^{r} \{g \cdot g_i^j \cdot g^{-1}\} \tag{5.1}$$

to be the union of all conjugates of the elements of cyclic subgroups generated by the elements $g_1, ..., g_r$. A pair of spherical systems of generators (T_1, T_2) of G is called *disjoint* if

$$\Sigma(T_1) \cap \Sigma(T_2) = \{1\}.$$

Next, we introduce unmixed and mixed ramification structures.

Definition 5.1.5. Let $A_1 = [m_{(1,1)}, .., m_{(1,r)}]$ and $A_2 = [m_{(2,1)}, .., m_{(2,s)}]$ be tuples of natural numbers with $2 \leq m_{(1,1)} \leq ... \leq m_{(1,r)}$ and $2 \leq m_{(2,1)} \leq ... \leq m_{(2,s)}$. An *unmixed ramification structure of type* (A_1, A_2) *for* G is a disjoint pair (T_1, T_2) of spherical systems of generators, such that T_1 has type A_1 and T_2 has type A_2.

The disjointness of the pair (T_1, T_2) in the definition of an unmixed ramification structure guarantees that G acts freely on the product $\mathcal{C}_{T_1} \times \mathcal{C}_{T_2}$ of the associated algebraic curves (see Section 5.3.3 and the references therein).

Definition 5.1.6. Let $A = [m_1, ..., m_r]$ be an r-tuple of natural numbers with $2 \leq m_1 \leq ... \leq m_r$. A *mixed ramification structure of type* A *for* G is a pair (H, T) where H is a subgroup of index 2 in G and $T = (g_1, ..., g_r)$ is an r-tuple of elements of G such that the following hold:

- T is a spherical system of generators of H of type A,
- for every $g \in G \setminus H$, the spherical systems T and gTg^{-1} are disjoint,
- for every $g \in G \setminus H$ we have $g^2 \notin \Sigma(T)$.

Definition 5.1.7. An *unmixed Beauville structure* is an unmixed ramification structure with two spherical systems (T_1, T_2) of generators of length 3, i.e., $r = 3$ and $s = 3$. A *mixed Beauville structure* is a mixed ramification structure with a spherical system T of generators of length 3, i.e., $r = 3$.

Remark 5.1.8. We note that if G has a mixed Beauville structure (H, T) of type A, then the index 2 subgroup H has an unmixed Beauville structure of type (A, A), by choosing the pair (T, gTg^{-1}) for an arbitrary $g \in G \setminus H$ and using the fact that H is normal in G. Moreover, there are corresponding unmixed and mixed Beauville surfaces $S_H = (\mathcal{C}_1 \times \mathcal{C}_2)/H$ and $S_G = (\mathcal{C}_1 \times \mathcal{C}_2)/G$, so that S_H is a 2-fold covering of S_G.

As [GP09b] states, the question of which finite groups admit an unmixed Beauville structure is deeply related to the question of which finite groups are quotients of certain triangle groups; a survey about this is given in [Con02].

Definition 5.1.9. An ordinary triangle group is a group given by the presentation,

$$T_{l,m,n} = \langle x, y, z | x^l, y^m, z^n, xyz \rangle.$$

The group is called,

1. *Hyperbolic* if $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$;
2. *Euclidean* if $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} = 1$;
3. *Spherical* if $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} > 1$.

5.1.2 From ramification structures to algebraic surfaces

In this section we explain how to construct an algebraic surface $S = (\mathcal{C}_{T_1} \times \mathcal{C}_{T_2})/G$ from a given finite group G with an unmixed ramification structure (T_1, T_2).

Let G be a finite group and $T = (g_1, ..., g_r)$ be a spherical system of generators with $m_i = \text{ord}(g_{\tau(i)})$. For $1 \leq i \leq r$, let $P_1, \ldots, P_r \in \mathbb{P}^1$ be a sequence of points ordered counterclockwise around a base point P_0 and $\gamma_i \in \pi(\mathbb{P}^1 - \{P_1, \ldots, P_r\}, P_0)$ be represented by a simple counterclockwise loop around P_i, such that $\gamma_1\gamma_2 \ldots \gamma_r = 1$.

We now recall the Riemann's existence theorem, see [Mir95, Fr80] for more information.

Theorem 5.1.10 (Riemann's Existence Theorem)**.** *There is a natural bijection between:*

- *Equivalence classes of holomorphic mappings $f : \mathcal{C} \to \mathbb{P}^1$, of degree n and with branch set $B_f \subset B$, (where $\mathcal{C}$ is a compact Riemann surface, and $f : \mathcal{C} \to \mathbb{P}^1$, $f' : \mathcal{C}' \to \mathbb{P}^1$ are said to be equivalent if there is a biholomorphism $g : C' \to C$ such that $f' = f \circ g$ and B is the set points $P_1, ..., P_r \in \mathbb{P}^1$).*

- *Conjugacy classes of monodromy homomorphisms $\mu : \pi_1(\mathbb{P}^1 - B) \to Sym(n)$ (here, $\mu \cong \mu'$ if and only if there is an element σ in $Sym(n)$ with $\mu(\gamma) = \sigma\mu'(\gamma)\sigma^{-1}$, for all simple closed curves γ).*

By Riemann's existence theorem, there exists a surjective homomorphism

$$\Phi : \pi(\mathbb{P}^1 - \{P_1, \ldots, P_r\}, 0) \to G$$

with $\Phi(\gamma_i) = g_i$ and a Galois covering $\lambda : \mathcal{C}_T \to \mathbb{P}^1$ with ramification indices equal to the orders of the elements $g_1, \ldots, g_r$. These data induce a well defined action of G on the curve $\mathcal{C}_T$, and by the Riemann-Huritz formula (see [Mir95, Fr80]), we have

$$g(\mathcal{C}_T) = 1 + \frac{|G|}{2}\left(r - 2 - \sum_{l=1}^{r} \frac{1}{m_l}\right). \tag{5.2}$$

Now, we assume that G admits an umixed ramification structure (T_1, T_2). This leads to a diagonal action of G on the product $\mathcal{C}_{T_1} \times \mathcal{C}_{T_2}$, and the disjointness of the two spherical systems of generators ensures that G acts freely on the product of curves. The associated algebraic surface S is the quotient $(\mathcal{C}_{T_1} \times \mathcal{C}_{T_2})/G$. By the Theorem of Zeuthen-Segre, we have for the topological Euler number

$$e(S) = 4\frac{(g(\mathcal{C}_{T_1}) - 1)(g(\mathcal{C}_{T_2}) - 1)}{|G|},$$

as well as the relations (see [Cat00, Theorem 3.4]),

$$\chi(S) = \frac{e(S)}{4} = \frac{K_S^2}{8},$$

where K_S^2 is the self intersection number of the canonical divisor and $\chi(S) = 1 + p_g(S) - q(S)$ is the holomorphic Euler-Poincaré characteristic of S. Assume that (T_1, T_2) is of the type (A_1, A_2) with $A_1 = [m_1, \ldots, m_r]$ and $A_2 = [n_1, \ldots, n_s]$. Then the above relations imply for the associated surface S that

$$\chi(S) = \frac{|G|}{4}\left(r - 2 - \sum_{l=1}^{r}\frac{1}{m_l}\right)\left(s - 2 - \sum_{l=1}^{s}\frac{1}{n_l}\right).$$

5.2 The group Γ and a 2-quotient with a mixed Beauville structure

5.2.1 The fundamental group Γ

We consider a simplicial complex $\mathcal{K}$, built from 7 triangles, following the relations given in the presentation of Γ. Note that all vertices of the triangles represent the same point in $\mathcal{K}$. Then, $\Gamma = \pi_1(\mathcal{K})$ is the fundamental group of the complex $\mathcal{K}$. Realising all triangles geometrically by equilateral Euclidean triangles, we can view the universal covering of $\mathcal{K}$ as a thick Euclidean building of type $\widetilde{A}_2$, with Γ being isomorphic to the group of covering transformations. The group Γ belongs to a family of groups introduced in [CMSZ93a] (and originally introduced in [EH88]), and is obviously presented by

$$\Gamma = \langle x_0, ..., x_6 \mid x_i x_{i+1} x_{i+3} \text{ for } i = 0, ..., 6\rangle,$$

where i, $i+1$ and $i+3$ are taken modulo 7.

In [PV08] the subgroup $H \subset \Gamma$ was considered, generated by x_0 and x_1, and the 2-quotients of this subgroup were employed for the explicit construction of expander graph families. We recall the following fact from [PV08]:

Proposition 5.2.1. *The group Γ is generated by x_0, x_1, x_2, and the subgroup H, generated by x_0, x_1 is an index two normal subgroup of Γ. Moreover, H has the presentation*

$$H = \langle x_0, x_1 \mid r_1, r_2, r_3\rangle,$$

with

$$\begin{aligned} r_1 &= x_1x_0x_1x_0x_1x_0x_1^{-3}x_0^{-3}, \\ r_2 &= x_1x_0^{-1}x_1^{-1}x_0^{-3}x_1^2x_0^{-1}x_1x_0x_1, \\ r_3 &= x_1^3x_0^{-1}x_1x_0x_1x_0^2x_1^2x_0x_1x_0. \end{aligned}$$

5.2.2 A group with a mixed Beauville structure

Let $G_{2,3}$ denote the maximal 2-quotient of Γ of 2-class 3. Similarly, let $H_{2,3}$ denote the maximal 2-quotient of the subgroup H of 2-class 3. $H_{2,3}$ is an index 2 subgroup of $G_{2,3}$. ($G_{2,3}$ and $H_{2,3}$ coincide with the groups $\texttt{SmallGroup}(256, 3679)$ and $\texttt{SmallGroup}(128, 36)$ in MAGMA Small Groups notation, see Section 4.4.) To simplify notation, we denote the images of x_0 and x_1 in $G_{2,3}$, again, by x_0 and x_1.

The quotient $G_{2,3}$ is of order $256 = 2^8$, and coincides with the non-abelian group (they call) $G(256, 2)$ in Bauer, Catanese and Grunewald [BCG08]. They constructed in [BCG08, Section 6.6] a mixed Beauville structure of type $[4, 4, 4]$ for this non-abelian group.

In our notation, we establish a mixed Beauville structure of type $A = [4, 4, 4]$ for the group $G_{2,3}$, by choosing $(H_{2,3}, T_1)$, where T_1 is the spherical system of generators (x_0, x_1, x) with $x = x_1^{-1}x_0^{-1}$. A second mixed Beauville structure of type A is given by the pair $(H_{2,3}, T_2)$ with $T_2 = (y_0, y_1, y)$, where $y_0 = x_0x_1^{-1}$ and $y_1 = x_1x_0x_1$ is another set of generators of $H_{2,3}$ and $y = y_1^{-1}y_0^{-1}$. Moreover, the disjoint pair (T_1, T_2) of spherical systems of generators is an unmixed Beauville structure of type (A, A) for the group $H_{2,3}$.

These facts were confirmed by MAGMA calculations, and lead to the study of Beauville structures for other maximal 2-quotients of the groups Γ and H.

5.3 Beauville structures for maximal 2-quotients

Before we present our results and conjectures, we fix some notation. We denote the maximal 2-quotient of 2-class k of Γ by $G_{2,k}$, and the maximal 2-quotient of 2-class k of H by $H_{2,k}$, *i.e.*

$$G_{2,k} := \texttt{pQuotient}(\Gamma, 2, k) \text{ and } H_{2,k} := \texttt{pQuotient}(H, 2, k).$$

For simplicity, we denote the images of x_0 and x_1 in $G_{2,k}$, again, by x_0 and x_1. We define $y_0 = x_0x_1^{-1}$, $y_1 = x_1x_0x_1$, and $x = x_1^{-1}x_0^{-1}$, $y = y_1^{-1}y_0^{-1}$, as well as the spherical systems of generators $T_1 = (x_0, x_1, x)$ and $T_2 = (y_0, y_1, y)$ for the groups $H_{2,k}$. For $x \in \mathbb{R}$, let $\lfloor x \rfloor$ be the largest integer smaller or equal to x. For an integer k,

let $k \bmod 3 \in \{0,1,2\}$ be the remainder under integer division by 3.

5.3.1 Which groups $H_{2,k}$ admit unmixed Beauville structures (T_1, T_2)?

Our MAGMA calculations show the following result for the maximal 2-quotients $H_{2,k}$ of 2-class $k \leq 64$:

Theorem 5.3.1. *Let* $3 \leq k \leq 63$, $r = \lfloor \log_2 k \rfloor + 1$ *and* $A = [2^r, 2^r, 2^r]$. *If* k *is not a power of* 2, *then* (T_1, T_2) *is an* unmixed Beauville structure *of type* (A, A) *for the group* $H_{2,k}$.

In the case that k is a power of 2, i.e., $k = 2^s$ for $s = 2, 3, \ldots, 6$, we found that $x_0^k = y_0^k$ and $x_1^k = y_1^k$, which means that (T_1, T_2) is not an unmixed Beauville structure of $H_{2,k}$. Moreover, the conjugacy classes of x_0^k and x_1^k in $G_{2,k}$ are trivial. Therefore, none of the pairs (T_1, gT_2g^{-1}) with $g \in G_{2,k}$ can be an unmixed Beauville structure of $H_{2,k}$.

We conjecture that all of the above results hold not only for $3 \leq k \leq 64$, but for all integers $k \geq 3$, thus providing infinitely many 2-groups admitting unmixed Beauville structures.

5.3.2 Which groups $G_{2,k}$ have mixed Beauville structures?

Since MAGMA calculations for mixed structures are far more intensive than for a particular unmixed structure, we confined our MAGMA calculations to all 2-quotients of 2-classes up to $k \leq 10$ and obtained the following result:

Theorem 5.3.2. *Let* $3 \leq k \leq 10$ *and* $r = \lfloor \log_2 k \rfloor + 1$. *If* k *is not a power of* 2, *then* $(H_{2,k}, T_1)$ *is a* mixed Beauville structure *of type* $[2^r, 2^r, 2^r]$ *for the group* $G_{2,k}$.

Again, we conjecture that this theorem holds for all integers $k \geq 3$ which are not powers of 2, thus providing infinitely many 2-groups admitting mixed Beauville structures.

5.3.3 What Beauville surfaces do these groups correspond to?

It is described, e.g., in [BCG05] or in [BCG06] and in general in Section 5.1.2 how to construct, for a given finite group G with a Beauville structure, a corresponding Beauville surface with minimal realisation $(\mathcal{C}_1 \times \mathcal{C}_2)/G$. We do not define some of the algebraic geometry terms but direct the reader to [Bea96] if they wish to learn more.

Let $T = (g_1, g_2, g_3)$ be a spherical system of generators of G of type $A = [a_1, a_2, a_3]$. Let $B = \{-1, 0, 1\} \subset \mathbb{P}^1$, and we fix the point $\infty \in \mathbb{P}^1$. Employing Riemann's existence theorem, this data is used to construct an explicit surjective homomorphism

$\pi_1(\mathbb{P}^1\backslash B, \infty) \to G$ with $\alpha \mapsto g_1, \beta \mapsto g_2, \gamma \mapsto g_3$, where α, β, γ are particularly chosen generators of $\pi_1(\mathbb{P}^1\backslash B, \infty)$ satisfying $\alpha\beta\gamma = 1$, and a corresponding Galois covering $\mathcal{C}_T \to \mathbb{P}^1$ with group G, ramified in the three points $-1, 0, 1 \in \mathbb{P}^1$, with ramification indices equal to the orders a_1, a_2 and a_3, respectively. The Riemann-Hurwitz formula yields for the genus $g(\mathcal{C}_T)$ of the curve $\mathcal{C}_T$,

$$2g(\mathcal{C}_T) - 2 = |G|(1 - \mu(A)), \tag{5.3}$$

where $\mu(A) = \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3}$. Assuming that G has an unmixed Beauville structure (T_1, T_2) of type (A_1, A_2), the corresponding Beauville surface is constructed as $S_G = (\mathcal{C}_{T_1} \times \mathcal{C}_{T_2})/G$. We have for the topological Euler number $e(S_G)$, by the Theorem of Zeuthen-Segre,

$$e(S_G) = 4\frac{(g(\mathcal{C}_{T_1}) - 1)(g(\mathcal{C}_{T_2}) - 1)}{|G|},$$

as well as the relations (see [Cat00, Theorem 3.4]),

$$\chi(S_G) = \frac{e(S_G)}{4} = \frac{K_{S_G}^2}{8},$$

where $K_{S_G}^2$ denotes the self intersection number of the canonical divisor.

Finally, since S_G is a surface of general type and $q(S_G) = 0$, we have

$$\chi(S_G) = 1 + p_g(S_G) = \frac{|G|}{4}(1 - \mu(A_1))(1 - \mu(A_2)). \tag{5.4}$$

These relations allow us to calculate all main invariants of Beauville surfaces corresponding to the groups $H_{2,k}$ and $G_{2,k}$, for which our MAGMA calculations showed the existence of unmixed and mixed Beauville structures:

1. Let $H_{2,k}$ have an unmixed Beauville structure of type (A, A) with $A = [2^r, 2^r, 2^r]$ and $r = \lfloor \log_2 k \rfloor + 1$. Let $S_{H_{2,k}} = (\mathcal{C}_1 \times \mathcal{C}_2)/H_{2,k}$ be the minimal realisation of an associated Beauville surface. Since $H_{2,k}$ is a group of order $2^{8\lfloor k/3 \rfloor + 3\cdot(k \bmod 3) - 1}$, we obtain from (5.3),

   $$g(\mathcal{C}_1) - 1 = g(\mathcal{C}_2) - 1 = 2^{8\lfloor k/3 \rfloor + 3\cdot(k \bmod 3) - r - 2}(2^r - 3),$$

   and from (5.4),

   $$1 + p_g(S_{H_{2,k}}) = \chi(S_{H_{2,k}}) = 2^{8\lfloor k/3 \rfloor + 3\cdot(k \bmod 3) - 2r - 3}(2^r - 3)^2.$$

2. Let $G_{2,k}$ have a mixed Beauville structure of type $A = [2^r, 2^r, 2^r]$ with $r = \lfloor \log_2 k \rfloor + 1$. Then $H_{2,k}$ admits unmixed Beauville structures of type (A, A)

by Remark 5.1.8, and we have a 2-fold covering $S_{H_{2,k}} \to S_{G_{2,k}}$ of associated Beauville surfaces. This implies

$$1 + p_g(S_{G_{2,k}}) = \chi(S_{G_{2,k}}) = \frac{1}{2}\chi(S_{H_{2,k}}) = 2^{8\lfloor k/3 \rfloor + 3\cdot(k \bmod 3) - 2r - 4}(2^r - 3)^2.$$

In the particular case $G_{2,3} \cong G(256, 2)$, we recover the results $g(\mathcal{C}_1) = g(\mathcal{C}_2) = 17$ and vanishing geometric genus $p_g(S_{G_{2,3}}) = 0$, in accordance with [BCG08].

Remark 5.3.3. [Con06] The group $H_{2,3}$ can be found as the 64^{th} quotient group of the hyperbolic triangle group

$$T_{4,4,4} = \langle x, y, z | xyz, x^4, y^4, z^4 \rangle,$$

of genus 17 defined by the presentation,

$$\langle x, y, z | xyz, x^4, y^4, z^4, (xzy^{-1})^2, (xz^{-1}y)^2, (x^{-1}zy)^2 \rangle,$$

using the computer program MAGMA.

The action is "Reflexible", that is there exists an involutory automorphism of the quotient that inverts the images of two of the three generators x, y and z.

5.4 Further Work

The above group Γ belongs to a family called *groups with special presentation*. These groups were introduced by Howie [How89] and are related to projective planes over finite fields.

It was proved in [EV10] that all groups with special presentation are just infinite (i.e. they are infinite groups all of whose non-trivial normal subgroups have finite index). A natural question arises: *Do any other groups with special presentations give rise to finite groups with particular ramification structures?*

Remark 5.4.1. The group G is also part of a family of groups defined by *triangle presentations* as defined in [CMSZ93a].

Future work could look at the above question. In fact, the beginnings of such a program has been started in [BBPV11b].

5.5 An infinite family of mixed Beauville surfaces

In the recent paper [BBPV14], we construct an infinite family of triples (G_k, H_k, T_k), where G_k are 2-groups of increasing order, H_k are index-2 subgroups of G_k, and T_k

are pairs of generators of H_k. We show that the triples $u_k = (G_k, H_k, T_k)$ are mixed Beauville structures if k is not a power of 2. Moreover, the associated Beauville surface $S(u_3)$ is real and, for $k > 3$ not a power of 2, the Beauville surface $S(u_k)$ is not biholomorphic to $\overline{S(u_k)}$.

Chapter 6

General non-abelian Beauville p-groups

This Chapter comprises work conducted under the supervision of N. Boston and B. Fairbairn, [BBF12].

In several places we shall refer to computer calculations that can easily be performed in Magma [BCP97] or GAP [GAP4]. In particular we will find it convenient to use the `SmallGroup(m,n)` notation that denotes the n^{th} group of order m in the small groups library, see Section 4.4 for references.

In addition, for economy of space, for each group presentation $\langle X|R\rangle$ stated we omit all commutator relations of the form $[a,b]=e$ from R for each pair $a,b\in X$ such that there does not exist a relator $[a,b]\neq e$ in R. We will indicate this by $\langle X|R\rangle_{\flat}$.

We will also state each spherical system of generators $T=(x,y,(xy)^{-1})$ simply as $(x,y)^{\dagger}$, this avoids confusion with commutators and saves writing the third generator which is always taken as $(xy)^{-1}$.

We now summarize the main results of this Chapter. In Section 6.1 we show that there exits a Beauville p-group for all groups of order $|G|=p^r$, $r\geq 2$. Sections 6.2 and 6.3 classify the non-abelian Beauville p-groups of order p^3 and p^4.

In the penultimate section, we examine the groups of order p^5 and prove the following theorem.

Theorem 6.0.1. *If $p>3$, then there exists at least $p+8$ Beauville groups of order p^5.*

From the analysis of the number of 2-generated groups of order p^5 we find the following consequence of the above theorem.

Corollary 6.0.2. *The proportion of 2-generated groups of order p^5 that are Beauville tends to 1 as p tends to infinity.*

For groups of order p^6 we find the following.

Theorem 6.0.3. *If $p > 3$, then there exist at least $p - 1$ 2-generated non-Beauville groups of order p^6.*

From the analysis of the number of 2-generated groups of order p^6 we find the following consequence of the above theorem.

Corollary 6.0.4. *The proportion of 2-generated groups of order p^6 that are Beauville does not tend to 1 as p tends to infinity.*

From [FGZ10] we have the following statement "it is very plausible that most 2-generated finite p-groups of sufficiently large order [are Beauville groups]". If we interpret that the word "most" from the statement to mean that the proportion of Beauville groups tends to 1 as p tends to infinity, then this statement would be true for groups of order p^5 but not for groups of order p^6.

Question 6.0.5. If $n > 6$, what is the behavior, as p tends to infinity, of the proportion of 2-generated groups which are Beauville?

Finally, through computational experimentation, we have the corollary of the combined results of this note.

Corollary 6.0.6. *The smallest non-abelian Beauville p-groups are*

1. *for $p = 2$,* `SmallGroup`*(2^7,36);*
2. *for $p = 3$, the group given by Example 6.4.1, of order 3^5;*
3. *for $p = 5$,* `SmallGroup`*(5^3,3);*
4. *for $p \geq 7$, the groups given by Lemma 6.2.1, of order p^3.*

6.1 Some general results

We first note a very easy lemma, which reduces the study of nilpotent Beauville groups to the study of Beauville p-groups.

Lemma 6.1.1. *Let G and G' be Beauville groups and let $\{(x_1, y_1)^\dagger, (x_2, y_2)^\dagger\}$ and $\{(x_1', y_1')^\dagger, (x_2', y_2')^\dagger\}$ be their respective Beauville structures. Suppose that for $i = 1, 2$*

$$gcd(o(x_i), o(x_i')) = gcd(o(y_i), o(y_i')) = 1.$$

Then $\{((x_1, x_1'), (y_1, y_1'))^\dagger, ((x_2, x_2'), (y_2, y_2'))^\dagger\}$ is a Beauville structure for the group $G \times G'$.

We now explicitly show that there is a non-abelian 2-generated non-Beauville group of order p^n for every $n \geq 3$ and for every prime p.

Lemma 6.1.2. *[BBF12, Lemma 9] The group*

$$G := \langle x, y | x^{p^n}, y^p, x^y = x^{p^{n-1}+1} \rangle$$

is a non-abelian 2-generated non-Beauville group of order p^{n+1} for every prime p and every $n > 1$.

Proof. [BBF12, proof of Lemma 9] Clearly G is non-abelian and 2-generated and a straightforward coset enumeration shows that the subgroup $\langle x \rangle$ has index p and so $|G| = p^{n+1}$. Now, $Z(G) = \langle x^p \rangle$ and every element outside the subgroup $\langle x^p, y \rangle$ has order p^n. Consequently, any generating set must contain at least one element of order p^n, but all such elements power up to $x^{p^{n-1}}$ (i.e. there exists $a \in \mathbb{N}$ such that, for $w \in G$, $w^a = x^{p^{n-1}}$), so G cannot have a Beauville structure. □

We remark that this lemma is a generalisation of [FJ09, Example 4A] which is the case $n = 2$.

Lemma 6.1.3. *[BBF12, Lemma 10] The group*

$$G := \langle x, y | x^{p^n}, y^{p^n}, x^y = x^{p+1} \rangle$$

is a non-abelian Beauville group of order p^{2n} for every prime $p \geq 5$ and every $n \geq 2$.

Proof. [BBF12, proof of Lemma 10] Clearly G is non-abelian and 2-generated and a straightforward coset enumeration shows that the subgroup $\langle x \rangle$ has index p^n and so $|G| = p^{2n}$. Let $p > 5$ be prime. We claim that $\{(x, y)^\dagger, (xy^2, xy^3)^\dagger\}$ is a Beauville structure in this case.

Now, every element of G can be written as $x^i y^j$ for some $0 \leq i, j \leq p^n - 1$. Furthermore, since $Z(G) = \langle x^{p^{n-1}}, y^{p^{n-1}} \rangle$ and so a necessary condition for two elements of G to be conjugate is that they power up to the same elements of $Z(G)$. A straightforward induction tells us that

$$(xy)^r = x^{1+(p+1)+(p+1)^2+\cdots+(p+1)^{r-1}} y^r.$$

An easy exercise in using geometric progressions and the binomial theorem tells us that for any prime p

$$1 + (1 + p) + \cdots + (1 + p)^{p^{n-1}-1} \equiv p^{n-1} \pmod{p^n}.$$

Combining these two identities gives $(xy)^{p^{n-1}} = x^{p^{n-1}}y^{p^{n-1}}$. Similar identities can be established for the elements xy^2, xy^3 and $(xy^2xy^3)y^{-5}y^5 = x^{1+(p+1)^2}y^5$, verifying that no powers of these elements are conjugate.

Finally we need show these pairs generate. Clearly $\langle x, y\rangle = G$ by definition. Since $(xy^2)^{-1}xy^3 = y$ and $xy^2y^{-2} = x$ so $G \leq \langle x, y\rangle \leq \langle xy^2, xy^3\rangle \leq G$.

Similar calculations in the case $p = 5$ show that $\{(x, y)^\dagger, (xy^2, xy^4)^\dagger\}$ is a Beauville structure. □

The above lemma has covered the groups of order an even power of a prime, p^{2n}. The next lemma covers the odd case, p^{2n+1}.

Lemma 6.1.4. *The group*

$$G := \langle x, y, z, \alpha_1, ..., \alpha_{n-1}, \beta_1, ..., \beta_{n-1} | x^{p^n}, y^{p^n}, z^p, [x, y] = z,$$

$$\alpha_i = x^{p^i}, \beta_i = y^{p^i} \text{ (for all } 1 \leq i \leq n-1) \rangle_\flat,$$

is a non-abelian Beauville group of order p^{2n+1} for $p \geq 5$ and $n \geq 2$.

Proof. For $p \geq 5$ and $n \geq 2$, it is clear that G is a 2-generated group by $(x, y)^\dagger$ and $(xy^2, xy^4)^\dagger$. Furthermore, we have distinct subgroups $\langle x\rangle, \langle y\rangle, \langle z\rangle$ of G of orders p^n, p^n, p respectively. As every element of G can be put in the form $x^iy^jz^k$, it follows that the order of G is p^{2n+1}.

We now claim the following is a Beauville structure $\{(x, y)^\dagger, (xy^2, xy^4)^\dagger\}$ for G. Since $\alpha_i, \beta_i \in Z(G)$ and $[x, y] = z$ we can construct the following Σ-sets,

$$\Sigma(x, y) = \{e\} \bigcup \left(\bigcup_{i=1}^{p^n-1} \{x^i, y^i, x^iy^i\}\langle z\rangle \right) \setminus \bigcup_{i=1}^{p^{n-1}-1} \bigcup_{j=1}^{p-1} \{x^{ip}z^j, y^{ip}z^j, x^{ip}y^{ip}z^j\},$$

and

$$\Sigma(xy^2, xy^4) =$$

$$\{e\} \bigcup \left(\bigcup_{i=1}^{p^n-1} \{x^iy^{2i}, x^iy^{4i}, x^{2i}y^{6i}\}\langle z\rangle \right) \setminus \bigcup_{i=1}^{p^{n-1}-1} \bigcup_{j=1}^{p-1} \{x^{ip}y^{2ip}z^j, x^{ip}y^{4ip}z^j, x^{2ip}y^{6ip}z^j\},$$

for this group. Here, we prefer to write the α_i's and β_j's in terms of powers of x^p and y^p respectively. Therefore, $\Sigma(x, y) \cap \Sigma(xy^2, xy^4) = \{e\}$. □

6.2 Groups of order $\leq p^3$

All groups of order p or p^2 are abelian for every prime p. Thus, by Theorem 4.1.3 the only Beauville group of order less than p^3 is $\mathbb{Z}_p \times \mathbb{Z}_p$ for $p > 3$. There are no abelian Beauville groups of order p^3.

The classification of groups of order p^3 is well-known; this result is due to [Hol93]. There are two non-abelian groups of order p^3. The first is of the form discussed in Lemma 6.1.2 and is thus not a Beauville group. The second is taken care of by the following, which is a special case of Lemma 6.1.4.

Lemma 6.2.1. *For any prime $p \geq 7$ the group*

$$G := \langle x, y, z | x^p, y^p, z^p, [x, y] = z \rangle_\flat$$

is a non-abelian Beauville group of order p^3 with Beauville structure $(T_1 = (x, y)^\dagger, T_2 = (xy^2, xy^3)^\dagger)$.

Proof. The group G is the extra special plus type group p_+^{1+2}. Since $xyx^{-1}y^{-1} = [x, y] = z$ we have that $xyx^{-1} = yz$ and since $C_G(y^i) = \langle y, z \rangle$ for $1 \leq i < p$ we see that the conjugates of y^i are precisely the elements $y^i z^j$ for $1 \leq j \leq p$. Similarly $C_G(g) = \langle g, z \rangle$ for all $g \in G \setminus Z(G)$.

Therefore, as

$$\Sigma(T_1) = \{e\} \bigcup_{j=1}^{p} \bigcup_{i=1}^{p-1} \{x^i z^j, y^i z^j, x^i y^i z^j\},$$

and

$$\Sigma(T_2) = \{e\} \bigcup_{j=1}^{p} \bigcup_{i=1}^{p-1} \{x^i y^{2i} z^j, x^i y^{3i} z^j, x^{2i} y^{5i} z^j\},$$

the condition $\Sigma(T_1) \cap \Sigma(T_2) = \{e\}$ is equivalent to:

$$(C_G(x) \cup C_G(y) \cup C_G(xy)) \cap (C_G(xy^2) \cup C_G(xy^3) \cup C_G(xy^2xy^3)) = Z(G).$$

Again, this can be shown to be equivalent to checking the equations $khk^{-1} \neq h$ for all $h \in T_1$ and $k \in T_2$. When showing this, we make use of the equation $(xy)^{-1}z = x^{p-1}y^{p-1}$ and $(xy^2xy^3)^{-1} = y^{p-5}x^{p-2}z^2$. We get the equations,

$$x^{-1}xy^2x = y^2x; \qquad x^{-1}xy^3x = y^3x;$$
$$y^{-1}xy^2y = yx^2z^2; \qquad y^{-1}xy^3y = y^2x^2z^3;$$
$$y^{-1}x^{-1}xy^2xy = y^2xz; \qquad y^{-1}x^{-1}xy^3xy = y^3xz;$$

$$x^{-1}y^{p-5}x^{p-2}z^2x = y^{p-5}x^{2p-4}z^{2+(p-5)(p-1)};$$
$$y^{-1}y^{p-5}x^{p-2}z^2y = y^{p-5}x^{p-2}z^p;$$
$$y^{-1}x^{-1}y^{p-5}x^{p-2}z^2xy = y^{p-5}x^{2p-2}z^{2p-1}.$$

As you can clearly see, some of the elements of $\{x, y, xy\}$ centralize some of the elements of $\{xy^2, xy^3, xy^2xy^3\}$ when $p \leq 5$. Therefore, the result holds for $p \geq 7$. □

Remark 6.2.2. The group given by Lemma 6.2.1 for $p = 7$ appears as the second group in a family of groups in [BBPV11b, Theorem 3.2]. There, it arises as a 7-quotient of a finite index subgroup of an infinite group with special presentation related to a finite projective planes.

6.3 Groups of order p^4

The classification of groups of order p^4 is well-known; this result is due to [Hol93]. We list the non-abelian 2-generated groups of order p^4 in Table 10.1 for p odd and Table 10.2 for $p = 2$. The only abelian Beauville group of order p^4 is $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ for $p > 3$.

The groups in Table 7.1 are stated to be Beauville or not in the final column. The groups in Table 7.2 are easily checked by computer to not be Beauville groups. We can state the above information in the following lemma.

Lemma 6.3.1. *[BBF12, Lemma 16] For any prime $p \geq 5$ the groups G_2 and G_7 are non-abelian Beauville groups of order p^4.*

For $p = 3$, the groups G_2 and G_7 are not Beauville groups.

6.4 Groups of order p^5

Computer calculations using MAGMA show that this is the first occurrence of a Beauville 3-group. This group is, in fact, the only Beauville group of order 3^5.

Name	Presentation	Beauville?
G_1	$\langle x,y \mid x^{p^3}, y^p, x^y = x^{1+p^2}\rangle$	No
G_2	$\langle x,y \mid x^{p^2}, y^{p^2}, x^y = x^{p+1}\rangle$	Yes $(p>3)$
G_3	$\langle x,y,z \mid x^{p^2}, y^p, z^p, [x,z]=y\rangle_\flat$	No
G_4	$\langle x,y,z \mid x^{p^2}, y^p, z^p, x^y = x^{p+1}, [x,z]=y\rangle_\flat$	No
G_5	$\langle x,y,z \mid x^{p^2}, y^p, z^p = x^p, x^y = x^{p+1}, [x,z]=y\rangle_\flat$	No
G_6	$\langle x,y,z \mid x^{p^2}, y^p, z^p = x^{p\alpha}, x^y = x^{p+1}, [x,z]=y\rangle_\flat$	No
G_7 $(p>3)$	$\langle w,x,y,z \mid w^p, x^p, y^p, z^p, [y,z]=x, [x,z]=w\rangle_\flat$	Yes $(p>3)$
G_8 $(p=3)$	$\langle x,y,z \mid x^9, y^3, z^3, [x,z]=y, [y,z]=x^3\rangle_\flat$	No

Table 6.1: The non-abelian 2-generated groups of order p^4, p odd. In the groups $G_3, ..., G_6$ and G_8, the presence of the relation $[x,z]=y$ shows that the group is 2-generated. In G_7 the presence of the relations $[y,z]=x$ and $[x,z]=w$ show that the group is 2-generated. In G_6 α is any quadratic non-residue (mod p).

Name	Presentation
G_1, G_2, G_3	as in Table 7.1
G_4	$\langle x,y \mid x^8, y^2, x^y = x^7\rangle$
G_5	$\langle x,y \mid x^8, y^2, x^y = x^3\rangle$
G_6	$\langle x,y \mid x^8, y^4, x^y = x^{-1}, x^4 = y^2\rangle$

Table 6.2: The non-abelian 2-generated groups of order 2^4.

Example 6.4.1. The group

$$\langle x,y,z,w,t \mid x^3, y^3, z^3, w^3, t^3, y^x = yz, z^x = zw, z^y = zt\rangle_\flat$$

is a non-abelian Beauville group of order 3^5 with Beauville structure given by $(S_1 = (x,y)^\dagger, S_2 = (xt, y^2w)^\dagger)$.

The computer program MAGMA was further used to explore the possible Beauville groups of order p^5, for $p>3$. The results of our computer experimentations are presented in Table 10.3. We note that there are no abelian Beauville groups of order p^5.

We observed that for each prime $5 \leq p \leq 19$ there are exactly $p+10$ Beauville groups of order p^5. The presentations for the $p+10$ groups are given below, seven H_i groups and $p+3$ $H_{i,j,k,l}$ groups. The remainder of this section is devoted to proving Theorem 6.0.1. We start by showing that five of the seven H_i groups are Beauville groups. We follow this, using the work of [Jam80, Section 4.5, part (6)], to analyze the family of non-isomorphic groups given by $H_{i,j,k,l}$.

p	n	$h(p)$	$g(p)$
2	-	19	0
3	3	29	1
5	2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 19, 20, 23, 30, 33	37	15
7	2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 21, 22, 25, 32, 37	41	17
11	2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 25, 26, 29, 36, 39	41	21
13	2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 27, 28, 31,38, 43	49	23
17	2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25,26, 31,32, 35, 42, 45	49	27
19	2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 33, 34, 37, 44, 49	53	29

Table 6.3: The groups `SmallGroup`(p^5,n) for $p \leq 19$ a prime that have Beauville structures. $h(p)$ (respectively $g(p)$) is the number of 2-generated (respectively Beauville) groups of order p^5.

Let $\mathbf{X} = \{x, y, z, w, t\}$ and set $H_i := \langle \mathbf{X} | \mathbf{R}_i \rangle_{\flat}$ for the below relations,

$$\mathbf{R}_1 = \{x^p = w, y^p = t, z^p, w^p, t^p, [y, x] = z\},$$

$$\mathbf{R}_2 = \{x^p, y^p, z^p, w^p, t^p, [y, x] = z, [z, x] = w, [z, y] = t\},$$

$$\mathbf{R}_3 = \{x^p = w, y^p = t, z^p, w^p, t^p, [y, x] = z, [z, x] = t\},$$

$$\mathbf{R}_4 = \{x^p = w, y^p = t^r, z^p, w^p, t^p, [y, x] = z, [z, x] = t\},$$

where r is taken as $2, 5, 6, 7, 6, 10$ for $p = 5, 7, 11, 13, 17, 19$ and

$$\mathbf{R}_5 = \{x^p = w, y^p = t, z^p, w^p, t^p, [y, x] = z, [z, x] = t, [z, y] = t\},$$

$$\mathbf{R}_6 = \{x^p, y^p, z^p, w^p, t^p, [y, x] = z, [z, x] = w, [w, x] = t\}$$

$$\mathbf{R}_7 = \{x^p, y^p, z^p, w^p, t^p, [y, x] = z, [z, x] = w, [z, y] = t, [w, x] = t\}.$$

Remark 6.4.2. It would be interesting to know how r, in the set of relations R_4, varies as a function of p.

We now look to [FJ09, Section 4] on lifting Beauville structures to extend the computational results for $p > 19$.

Definition 6.4.3. Let G be a finite group with a normal subgroup N. An element g of G is faithfully represented in G/N if $\langle g \rangle \cap N = \{e\}$.

If $T = \{g_1, ..., g_k\}$ is a k-tuple of elements of G, we say that this k-tuple is faithfully

represented in G/N if $\langle g_i \rangle \cap N = \{e\}$ for $1 \leq i \leq k$.

Lemma 6.4.4. *[FJ09, Lemma 4.2] Let G have generating triples $\{x_i, y_i, z_i\}$ with $x_i y_i z_i = e$ for $i = 1, 2$ and a normal subgroup N such that at least one of these triples is faithfully represented in G/N.*

If the images of these triples corresponds to a Beauville structure for G/N, then these triples correspond to a Beauville structure for G.

We can now make the following conclusions for some of the group structures $H_i = \langle \mathbf{X} | \mathbf{R}_i \rangle_\flat$.

Lemma 6.4.5. *Let $H_i = \langle \mathbf{X} | \mathbf{R}_i \rangle_\flat$ for $i = 2, 6, 7$ and $p \geq 5$ a prime. Then, H_i is a Beauville group of order p^5.*

Proof. Firstly, for $p = 5$ MAGMA calculations show that the groups H_i for $i = 2, 6, 7$ have Beauville structures corresponding to $\{(x, y)^\dagger, (xy^2, xy^4)^\dagger\}$.

Secondly, let $p \geq 7$. For each group H_i the center $Z_i = Z(H_i)$ is given by the subgroup $\langle t, w \rangle$ and $(x, y)^\dagger, (xy^2, xy^3)^\dagger$ are two generating sets for the groups H_i for $i = 2, 6, 7$. The quotient group H_i/Z_i is isomorphic to the group G given in Lemma 6.2.1. Clearly, the images of x, y and xy in H_i/Z_i are faithfully represented (in the sense of Definition 6.4.3) and correspond with the Beauville structure $\{(x, y)^\dagger, (xy^2, xy^3)^\dagger\}$ for the group G.

Thus, by Lemma 6.4.4 we see that the Beauville structure $\{(x, y)^\dagger, (xy^2, xy^3)^\dagger\}$ lifts to a Beauville structure for the groups H_i for $i = 2, 6, 7$. □

Lemma 6.4.6. *Let $H_1 = \langle \mathbf{X} | \mathbf{R}_1 \rangle_\flat$ and $p \geq 5$ a prime. Then, H_1 is a Beauville group of order p^5.*

Proof. By Lemma 6.1.4, with $n = 2$, we see that the groups H_1 have Beauville structures corresponding to $\{(x, y)^\dagger, (xy^2, xy^4)^\dagger\}$. □

Lemma 6.4.7. *Let $H_5 = \langle \mathbf{X} | \mathbf{R}_5 \rangle_\flat$ and $p \geq 5$ a prime. Then, H_5 is a Beauville group of order p^5.*

Proof. We claim that the groups H_2 for $p \geq 5$ have Beauville structures corresponding to $\{(x, y)^\dagger, (xy^2, xy^4)^\dagger\}$.

It is clear that $\{x, y\}$ and $\{xy^2, xy^4\}$ are generating sets for H_5. Now, given that $x^p = w$, $y^p = t$, $[x, y] = z$, $[z, x] = [z, y] = t$ and the center $Z(H_5) = \langle w, t \rangle$ we see that

$$\Sigma(x, y) =$$

$$\{e\} \bigcup \left(\bigcup_{i=1}^{p^2-1} \{x^i, y^i, x^i y^i\} \langle z \rangle \langle y^p \rangle \right) \setminus \bigcup_{i,j,k=1}^{p-1} \{x^{ip} y^{jp} z^k, y^{ip} y^{jp} z^k, x^{ip} y^{ip} y^{jp} z^k\},$$

and

$$\Sigma(xy^2, xy^4) = \{e\} \bigcup \left(\bigcup_{i=1}^{p^2-1} \{x^i y^{2i}, x^i y^{4i}, x^{2i} y^{6i}\} \langle z \rangle \langle y^p \rangle \right)$$

$$\setminus \bigcup_{i,j,k=1}^{p-1} \{x^{ip} y^{2ip} y^{jp} z^k, x^{ip} y^{4ip} y^{jp} z^k, x^{2ip} y^{6ip} y^{jp} z^k\}.$$

We prefer to write w in terms of x^{ip} and t in terms of y^{ip} for $0 \leq i \leq p-1$. Therefore, $\Sigma(x,y) \cap \Sigma(xy^2, xy^4) = \{e\}$. □

We are now left with the groups given by relations $\mathbf{R}_i$ for $i = 3, 4$. We cannot lift Beauville structures from groups of order $< p^5$ to the groups H_i for $i = 3, 4$ as any normal subgroup N_i of H_i would decrease the order of the generators x, y. Thus, x, y would not be faithfully represented in H_i/N_i.

We now have the following groups for selected values of $i, j, k, l \in \{0, ..., p-1\}$. We find $p+3$ non-isomorphic groups for $5 \leq p \leq 19$ give rise to Beauville p-groups with the following presentations,

$$H_{i,j,k,l} := \langle x, y, z, w, t | x^p = w^i t^j, y^p = w^k t^l, z^p, w^p, t^p, [x,y] = z, [x,z] = w, [y,z] = t \rangle_\flat.$$

These groups correspond to the groups `SmallGroup`(p^5, n) for $7 \leq n \leq p+9$, as given by the MAGMA small groups library.

From [Jam80, Section 4.5, part (6)], the group structures for p-groups of order p^5 for $p > 3$ are listed. The groups having the structure of $H_{i,j,k,l}$ are therefore given in the classification. We can therefore state the following lemma which is a consequence of the classification of groups of order p^5.

Lemma 6.4.8. *If $p > 3$ a prime, then there are $p+7$ non-isomorphic groups of the following form,*

$$H_{i,j,k,l} := \langle x, y, z, w, t | x^p = w^i t^j, y^p = w^k t^l, z^p, w^p, t^p, [x,y] = z, [x,z] = w, [y,z] = t \rangle_\flat$$

where $i, j, k, l \in \{0, ..., p-1\}$.

Proof. From [Jam80, Section 4.5, part (6)], we see that there are

$$1 + \frac{1}{2}(p-1) + 2 + 1 + \frac{1}{2}(p-1) + 1 + 2 + 1 = p + 7$$

groups of this form. □

We are now in a position to prove Theorem 6.0.1, which was stated in the Introduction. It is convenient to note that all the groups $H_{i,j,k,l}$ have center $Z_{i,j,k,l} = \langle w, t \rangle$ and $H_{i,j,k,l}/Z_{i,j,k,l} \cong G$, the group given by Lemma 6.2.1.

Proof of Theorem 6.0.1: Firstly, by Lemmas 6.4.5, 6.4.6 and 6.4.7 we have five Beauville groups for each prime $p > 3$.

Secondly, we consider the $p + 7$ non-isomorphic groups $H_{i,j,k,l}$ given by Lemma 6.4.8. We note that the group given by H_2 corresponds to $H_{0,0,0,0}$ and thus we have $p + 6$ non-isomorphic groups of the form $H_{i,j,k,l}$ to account for.

The groups corresponding to $\Phi_6(21111)b_r$ in [Jam80, Section 4.5, part (6)] cannot admit a Beauville structure as $x^p = e$, $y^p = w^r$ where $r = 1$ or ν (the smallest positive integer which is a non-quadratic residue modulo p). The group given by $\Phi_6(21111)a$ in [Jam80, Section 4.5, part (6)] cannot admit a Beauville structure as $x^p = w$, $y^p = e$. We are therefore left with $p + 3$ non-isomorphic groups to analyse.

The remaining $p + 3$ groups $H_{i,j,k,l}$ have non-trivial words $u(w,t), v(u,t)$ such that $x^p = u(w,t)$ and $y^p = v(w,t)$. As the words u, v are made up of elements of the center $Z_{i,j,k,l}$ of the groups $H_{i,j,k,l}$ and the order of the elements x, y is p^2, we see that the remaining $p + 3$ groups satisfy the criteria $\Sigma(x,y) \cap \Sigma(xy^2, xy^4) = \{e\}$ for $p > 3$. That is, each element of the form $x^a y^b z^c$ (with both $a \neq 0$ and $b \neq 0$) is conjugate to elements of the form $x^a y^b z^d s(w,t)$, where $s(w,t)$ is a word in w, t. Therefore, $\{(x,y)^\dagger, (xy^2, xy^4)^\dagger\}$ is a Beauville structure for the remaining $p + 3$ groups. The result them follows. □

We see for $5 \leq p \leq 19$ that the number of groups found to have Beauville structures is $p + 10$. From the work above, we are led to make the following conjecture.

Conjecture 6.4.9. For all $p \geq 5$, the number of Beauville p-groups of order p^5 is given by $g(p) = p + 10$.

In particular, H_3 and H_4 are Beauville groups for $p \geq 5$.

In the preceding paragraphs we produced $p + 8$ groups of order p^5 that admit a Beauville structure.

For groups of order p^5, the number of 2-generated groups is approximately half of the total number of groups. We see from [Jam80], that the exact number of 2-generated p-groups of order p^5 for $p \geq 5$ is given by

$$h(p) = p + 26 + 2\gcd(p-1,3) + \gcd(p-1,4).$$

Thus, $h(p) \sim p$ as $p \to \infty$. The function $h(p)$ is an obvious upper bound for the number of Beauville groups of order p^5. Since $p + 36 \geq h(p) > g(p) \geq p + 8$ we get that $g(p) \sim p$ as $p \to \infty$ and so,

$$\lim_{p\to\infty} \frac{g(p)}{h(p)} = 1.$$

Thus, the proportion of 2-generated groups of order p^5 which are Beauville tends to

1 as p tends to infinity, which establishes Corollary 6.0.2.

6.5 Remarks on Groups of order p^6

For groups of order p^6, we used MAGMA to determine that there are no Beauville 2-groups and only three Beauville 3-groups. These groups correspond to the groups `SmallGroup`(3^6, n) for $n = 34, 37, 40$.

Remark 6.5.1. It is interesting to note that Corollary 6.0.4 also holds for non-abelian 2-generated groups of order p^6 since there are only 3 abelian ones.

For $p > 3$, we would like an asymptotic result for groups of order p^6, similar to that in Section 6.4 for p^5. Using [NOV04, Theorem 2 and Table 1], we see that there are in total

$$f(p) = 10p + 62 + 14\gcd(3, p-1) + 7\gcd(4, p-1) + 2\gcd(5, p-1)$$

2-generated groups of order p^6 for $p > 3$ a prime. Thus, $f(p) \sim 10p$ as $p \to \infty$.

From [NOV04, Theorem 2], the family of groups of order p^6 given by "3) $\langle a, b | b^p$, *class* $2\rangle$" give rise to $p + 15$ non-isomorphic groups (see [NOV04, Table 1]). One can generate these group presentations for each p a prime by the following MAGMA code:

```
> G:=Group<a,b|b^p>;
> P:=pQuotient(G,p,2);
> D:=Descendants(P: OrderBound := p^6);
> D := [d: d in D | #d eq p^6];
```

Each of the groups contained in D is 2-generated, say by x and y. We find that, for each p a prime, there exists a family of non-isomorphic groups contained in D given by the following presentations,

$$K_r = \langle x, y, z, u, v, w | x^p = u, y^p = w^r, z^p, u^p = v, v^p, w^p, [y, x] = z, [z, x] = v, [z, y] = w \rangle_\flat,$$

for $r = 1, ..., p-1$.

It follows that all of the $p - 1$ groups have $o(x) \neq o(y)$. You can clearly see, given the above group structures, if $o(x) \neq o(y)$ then K_r does not have a Beauville structure (this is similar to the third paragraph of the proof of Theorem 6.0.1, Section 6.4). That is, any second set of generators one tries to construct will have elements of the form $x^a y^b$ and so if $o(x) \neq o(y)$ we will have $\Sigma(x, y) \cap \Sigma(x^a y^b, x^c y^d) \neq \{e\}$. Therefore, we obtain a family of $p - 1$ 2-generated non-Beauville groups of order p^6, which proves Theorem 6.0.3 and establishes Corollary 6.0.4.

Index

Bibliography

[AS74] M. Anshel and P. Stebe, "The solvability of the conjugacy problem for certain HNN groups", *Bull. Amer. Math. Soc.*, **80** (2) (1974) 266–270.

[Bar11] N. Barker, "An algebraic approach to centralizers and the conjugacy problems in the Higman-Thompson group $G_{2,1}$", submitted (2011).

[BBPV11a] N. Barker, N. Boston, N. Peyerimhoff and A. Vdovina, "New examples of Beauville surfaces", to appear in *Monatsh. Math.* DOI: 10.1007/s00605-011-0284-6 (2011). Monatsh. Math. 166, no. 3-4, 319–327 (2012).

[BBPV11b] N. Barker, N. Boston, N. Peyerimhoff and A. Vdovina, "Regular algebraic surfaces isogenous to a higher product constructed from group representations using projective planes", arXiv:1109.6053v1 [math.GR] (2011).

[BBF12] N. Barker, N. Boston and B. Fairbairn, "A note on Beauville p-groups", accepted *Exper. Math.* DOI:10.1080/10586458.2012.669267 (2012) .

[BBPV14] N. Barker, N. Boston, N. Peyerimhoff and A. Vdovina, "An Infinite Family of 2-Groups with Mixed Beauville Structures", accepted *Int Math Res Notices* DOI:10.1093/imrn/rnu045 (2014) .

[BCG05] I.C. Bauer , F. Catanese, F. Grunewald, "Beauville surfaces without real structures", Geometric methods in algebra and number theory, *Progr. Math.*, **235**, Birkhauser Boston, Boston, MA, pp. 1-42, (2005)

[BCG06] I.C. Bauer , F. Catanese, F. Grunewald, "Chebycheff and Belyi polynomials, dessins d'enfants, Beauville surfaces and group theory", *Mediterr. J. Math.*, **3**(2), 121-146, (2006)

[BCG08] I.C. Bauer , F. Catanese, F. Grunewald, "The classification of surfaces with $p_g = q = 0$ isogenous to a product of curves", *Pure Appl. Math. Q.*, **4**(2), part 1, 547-586, (2008)

[BCG10] I.C. Bauer, F. Catanese, R. Pignatelli, "Surfaces of general type with geometric genus zero: a survey", arXiv:1004.2583v1, (2010)

[Bea78] A. Beauville, "Surfaces algébriques complexes", Société Mathématique de France, Paris, Avec une sommaire en anglais, Astérisque, no. 54, (1978)

[Bea96] A. Beauville, "Complex Algebraic Surfaces", Cambridge University Press, (1996).

[BBO02] H. U. Besche, B. Eick and E. O'Brien, "A millennium project: constructing Small Groups", *Internat. J. Algebra Comput.* 12, 623 - 644 (2002).

[SmallGroups] H. U. Besche, B. Eick and E. O'Brien, Small Groups Library, `http://www.icm.tu-bs.de/ag_algebra/software/small/`.

[Bel80] G. V. Beyli, "On Galois extensions of a maximal cyclotomic field", *Izv. Akad. Nauk SSSR* 43 (1979) 269Ð276 (Russian); Math. USSR Izvestiya 14 (1980), 247–256 (English translation).

[BGG11] C. Bleak, A. Gordon, G. Garrett, H. Newfield-Plunkett-Bowman, E. Sapir, F. Matucci and J. Hughes, "Centralizers in R.Thompson's group V_n", arXiv:1107.0672v3 [math.GR] (2011).

[BO93] R. V. Book and F. Otto, "String-rewriting Systems", Springer, (1993).

[BCP97] W. Bosma, J. Cannon, C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.*, **24**(3-4), 235-265, (1997)

[Bri97] M. Brin, "The Chameleon Groups of Richard J. Thompson: Automorphisms and Dynamics", *Pub. Math. IHES* 84 (1997) 5-33.

[Brin04] M.G. Brin, "Higher dimensional Thompson groups", *Geom. Dedicata*, **108** (2004) 163-192.

[Cam32] L. Campedelli, "Sopre alcuni piani doppi notevoli can curve di diramazione del decimo ordine", *Atti. Acad. Naz. Lincei* **15**, (1932) 536–542.

[CFP96] J.W. Cannon, W.J. Floyd and W.R. Parry, "Introductory notes on Richard Thompson's groups", *Enseign. Math.*, (2) **42**(3-4) (1996) 215-256.

[CMSZ93a] D.I. Cartwright, A.M. Mantero, T. Steger, A. Zappa, "Groups acting simply transitively on the vertices of a building of type $\widetilde{A}_2$, I", *Geom. Dedicata*, **47**(2), 143-166, (1993).

[CMSZ93b] D.I. Cartwright, A.M. Mantero, T. Steger and A. Zappa, "Groups acting simply transitively on the vertices of a building of type $\widetilde{A}_2$, II", *Geom. Dedicata* **47**(2) (1993), 167–223.

[Cat00] F. Catanese, "Fibred surfaces, varieties isogenous to a product and related moduli spaces", *Amer. J. Math.* **122**(1), 1-44, (2000)

[Cohn81] P. M. Cohn, "Universal Algebra". Mathematics and its Applications, 6, D. Reidel Pub. Company, (1981).

[Cohn91] P. M. Cohn, "Algebra, Volume 3". J. Wiley, (1991).

[Com77] L. P. J. Comerford, A note on power-conjugacy, *Houston J. Math.* 3 (1977), no. 3, 337—341.

[Con02] M. Conder, "Hurwitz groups with given centre", *Bull. London Math. Soc.* **34**(6), 725-728, (2002).

[Con06] M. Conder, "Quotients of triangle groups acting on surfaces of genus 2 to 101", `http://www.math.auckland.ac.nz/ conderTriangleGroupQuotients101.txt`.

[Dehn1911] M. Dehn, "Uber unendliche diskontinuierliche Gruppen", *Math. Ann.*, 1911.

[EH88] M. Edjvet, J. Howie, "Star graphs, projective planes and free subgroups in small cancellation groups", *Proc. London Math. Soc.* (3) **57**(2), 301-328, (1988).

[EV10] M. Edjvet and A. Vdovina, "On the SQ-universality of groups with special presentations", *J. Group Theory* **13**(6) (2010), 923–931.

[Enr1896] F. Enriques, "Introduzione alla geometria sopra le superficie algebriche", Memorie della Societa' Italiana delle Scienze (detta "dei XL"), s.3, to. X, (1896), 1-81.

[Fa10] B. Fairbairn, "Some exceptional Beauville structures", arXiv:1007.5050 (2010).

[FMP10] B. Fairbairn, K. Magaard, C. Parker, "Generation of finite simple groups with an application to groups acting on Beauville surfaces", arXiv:1010.3500 (2010).

[Fr80] M. Fried, "Exposition on an arithmetic-group theoretic connection via the Riemann's Existence theorem", *Proceedings of the symposium in Pure Mathematics*, Vol 37, 571–602 (1980)

[FG10] Y. Fuertes, G. González-Diez, "On Beauville structures on the groups S_n and A_n", *Math. Z.* **264**(4), 959-968, (2010)

[FGZ10] Y. Fuertes, G. González-Diez, A. Jaikin-Zapirain, "On Beauville surfaces", *Groups Geom. Dyn.* 5(1) (2011) 107-119.

[FJ09] Y. Fuertes, G. A. Jones, "Beauville surfaces and finite groups", *J. Algebra* **340** (2011), 13–27.

[GAP4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008,(`http://www.gap-system.org`).

[Gar10] S. Garion, "On Beauville Structures for $PSL(2,q)$", arXiv:1003.2792v1, (2010).

[GLL10] Garion, S., Larsen, M., Lubotzky, A.: Beauville surfaces and finite simple groups. arXiv:1005.2316v1[math.GR], (2010).

[GP09a] S. Garion, M. Penegini, "New Beauville surfaces and finite simple groups", arXiv:0910.5402v3, (2011).

[GP09b] S. Garion, M. Penegini, "Beauville surfaces, moduli spaces and finite groups", arXiv:1107.5534, (2011).

[Go35] L. Godeaux, "Les involutions cycliques qppartenant á une surface algébrique", *Actual. Sci. Ind.*, **270**, Herman, Paris, (1935).

[GJT11] G. González-Diez, G. A. Jones, D. Torres-Teigell, "Beauville surfaces with abelian Beauville group", arXiv:1102.4552, (2011).

[GM10] R. Guralnick, G. Malle, "Simple groups admit Beauville structures", arXiv:1009.6183, (2011).

[Hig74] G. Higman, "Finitely presented infinite simple groups", *Notes on Pure Mathematics*, Vol. 8 (1974).

[Hol93] O. Hölder, "Die Gruppen der Ordnung p^3, pq^2, pqr, p^4", *Math. Ann.* 43 (1893), 301-412.

[How89] J. Howie, "On the SQ-universality of $T(6)$-groups", *Forum Math.* **1**(3) (1989), 251–272.

[Jam80] R. James, "The Groups of Order p^6 (p an Odd Prime)", *Math. Comp.* 34, No. 150 (1980), 613-637.

[JS94] G. A. Jones and D. Singerman, "Maps, hypermaps and triangle groups", in The Grothendieck Theory of Dessins d'Enfants (L. Schneps ed.), *London Math. Soc. Lecture Note Ser.* 200 (1994), 115-145.

[JS96] G. A. Jones and D. Singerman, "Belyi functions, hypermaps and Galois groups", *Bull. London Math. Soc.* 28 (1996), 561-590.

[L-GM02] C. R. Leedham-Green and S. McKay, "The structure of groups of prime power order", LMS Monographs, New Series, 27. Oxford Science Publications. Oxford University Press, Oxford, (2002) xii+334.

[Lip66] S. Lipschutz, "Generalisation of Dehn's result on the conjugacy problem", *Proc. Amer. Math. Soc.*, **17** (1966) 759–762.

[Lot83] M. Lothaire, "Combinatorics on Words", Addison-Wesley, Advanced Book Program, World Science Division, (1983).

[LSV05] A. Lubotzky, B. Samuels and U. Vishne, "Explicit construction of Ramanujan complexes of type $\widetilde{A}_d$", *European J. Combin.* 26(6) (2005) 965–993.

[MKS04] W. Magnus, A. Karrass and D. Solitar, "Combinatorial group theory: Presentations of groups in terms of generators and relations", 2nd edition, Dover Publications, (2004).

[Mill71] C.F.Miller III, "On group-theoretic decision problems and their classification", *Annals Of Mathematics Studies* 68, Princeton University Press, 1971.

[Mir95] R. Miranda, "Algebraic curves and Riemann surfaces", Graduate Studies in Mathematics, 5, American Mathematical Society, Providence, RI, (1995).

[NOV04] M. F. Newman, E. A. O'Brien and M. R. Vaughan-Lee, "Groups and nilpotent Lie rings whose order is the sixth power of a prime", J. Algebra 278 (2004), no. 1, 383–401.

[Pride08] S. J. Pride, "On the residual finiteness and other properties of (relative) one-relator groups", *Proc. Amer. Math. Soc.* **136** (2) (2008) 377–386.

[Rose78] J. S. Rose, "A course on Group Theory", Cambridge University Press, (1978).

[SD10] O.P. Salazar-Diaz, "Thompson's group V from a dynamical viewpoint", *Internat. J. Algebra Comput.*, 1, 39-70, 20, (2010).

[Ser96] F. Serrano, "Isotrivial fibred surfaces", *Ann. Mat. Pura Appl. (4)* **171** (1996), 63–81.

[Sin01] D. Singerman. "Riemann surfaces, Bely functions and hypermaps", in Topics on Riemann surfaces and Fuchsian groups, ed. by E.Bujalance, A.F.Costa and E. Martinez London Math.Soc. Lecture Note series,287. (2001), CUP.

[Syl1872] L. Sylow, "Théorémes sur les groupes de substitutions", *Math. Ann. 5*, (1872), 584–594.

[PV08] N. Peyerimhoff and A. Vdovina, "Cayley graph expanders and groups of finite width", to appear in *J. Pure and Applied Algebra* (2011).

[Rob96] D. J. S. Robinson, A course in the theory of groups, 2nd ed., Graduate Texts in Math., vol. 80, Springer, New York, (1996).

[Tho] R.J. Thompson, unpublished notes.

http://www.math.binghamton.edu/matt/thompson/index.html